Ultimate Protection Suite

Manuale utente

Marchio registrato e copyright

Marchio registrato

Windows è un marchio registrato di Microsoft Corporation negli Stati Uniti e in altri paesi.
Tutti gli altri marchi o nomi di prodotti sono marchi registrati del legittimo proprietario.
I marchi protetti non sono contrassegnati come tali in questo manuale. Ciò tuttavia non significa che possano essere liberamente utilizzati.

Note sul Copyright

Per Avira Ultimate Protection Suite viene utilizzato il codice di terzi. Ringraziamo i possessori di copyright per aver messo a disposizione il proprio codice.
Informazioni dettagliate sul copyright sono disponibili nella Guida in linea di Avira Ultimate Protection Suite in "Third Party Licenses".

Contratto di licenza con l’utente finale (EULA)

https://www.avira.com/it/license-agreement

Tutela della privacy

https://www.avira.com/it/general-privacy

Indice

1. Introduzione

Il prodotto Avira in uso permette di proteggere il computer da virus, worm, trojan, adware e spyware e altri rischi. In breve, in questa guida si parla di virus, malware (software dannosi) e programmi indesiderati.

La guida descrive l'installazione e il funzionamento del programma.

Sul nostro sito Web sono disponibili diverse opzioni e ulteriori informazioni:

http://www.avira.com/it

Sul sito Web di Avira è possibile:

- visualizzare informazioni relative ad altri programmi Avira per il desktop
- scaricare i programmi Avira per il desktop più recenti
- scaricare le guide del prodotto più recenti in formato PDF
- scaricare tool gratuiti per l'assistenza e la riparazione
- accedere alla completa Knowledge Base e alle domande frequenti per la risoluzione dei problemi
- visualizzare gli indirizzi dell'assistenza specifici per ogni paese.

Il team di Avira

1.1 Simboli ed evidenziazioni

Vengono utilizzati i seguenti simboli:

Simbolo/Definizione	Spiegazione
✓	Indica un requisito che deve essere soddisfatto prima che sia eseguita un'operazione.
▸	Indica un'operazione da eseguire.
↳	Indica un evento scaturito dall'operazione precedente.
Avviso	Indica un avviso di pericolo di una significativa perdita di dati.

Nota	Indica un messaggio con informazioni particolarmente importanti o un suggerimento che agevola la comprensione e l'uso del prodotto Avira.

Vengono utilizzate le seguenti evidenziazioni:

Evidenziazione	Spiegazione
Corsivo	Nome del file o percorso.
	Elementi dell'interfaccia software che vengono visualizzati (ad esempio sezione della finestra o messaggio di errore).
Grassetto	Elementi dell'interfaccia software su cui è possibile fare clic (ad es. voci di menu, rubriche, campi di opzione o pulsanti).

2. Informazioni sul prodotto

In questo capitolo è possibile consultare tutte le informazioni rilevanti per l'acquisto o l'utilizzo del prodotto Avira:

- vedere capitolo: Prestazioni
- vedere capitolo: Requisiti di sistema
- vedere capitolo: Licenza e aggiornamento
- vedere capitolo: Gestione delle licenze

I prodotti Avira offrono tool completi e flessibili per garantire una protezione affidabile del computer da virus, malware, programmi indesiderati e altri pericoli.

- Nota:

Avviso
La perdita di dati importanti ha spesso conseguenze drammatiche. Nemmeno il miglior programma antivirus può offrire una protezione al 100% contro la perdita di dati. Si consiglia di eseguire regolarmente copie di sicurezza (backup) dei dati.

Nota
Un programma in grado di proteggere il computer da virus, malware, programmi indesiderati e altri pericoli può essere affidabile ed efficace solo se aggiornato regolarmente. Si consiglia di garantire l'aggiornamento del prodotto Avira con gli aggiornamenti automatici. Configurare il programma in modo adeguato.

2.1 Prestazioni

Il prodotto Avira offre le seguenti funzionalità:

- Control Center per il monitoraggio, l'amministrazione e la gestione dell'intero programma
- Configurazione centrale con configurazione semplice in modalità esperto oppure standard e dotata di guida sensibile al contesto
- System Scanner (On-Demand Scan) con scansione di tutti i tipi noti di virus e malware gestita dal profilo e configurabile
- Integrazione nella funzionalità di controllo dell'account utente di Windows per poter eseguire operazioni per le quali sono necessari i diritti di amministratore.
- Real-Time Protection (On-Access Scan) per il costante monitoraggio di tutti gli accessi ai file

- Componente ProActiv per il monitoraggio permanente di azioni eseguite dai programmi (solo per sistemi a 32 bit)
- Mail Protection (scanner POP3, scanner IMAP e scanner SMTP) per il controllo permanente delle email alla ricerca di virus e malware, inclusa la scansione degli allegati dei messaggi email
- Avira SearchFree Toolbar, una barra degli strumenti di ricerca integrata nel web browser per eseguire ricerche in modo rapido e semplice. La barra degli strumenti contiene anche i widget delle funzioni più importanti per la navigazione su Internet.
- Web Protection per il controllo di dati e file provenienti da Internet tramite il protocollo HTTP (controllo delle porte 80, 8080, 3128)
- Il componente Protezione dei bambini è provvisto di filtri basati sui ruoli per filtrare pagine Web indesiderate e per limitare il tempo di utilizzo di Internet.
- Avira Free Android Security è un'app che protegge i dispositivi da furto e/o smarrimento. L'app aiuta l'utente a ritrovare il dispositivo mobile in caso di smarrimento o peggio ancora in caso di furto. Quest'applicazione permette inoltre di bloccare le telefonate o gli SMS in arrivo. Avira Free Android Security protegge i telefoni cellulari e gli smartphone basati sul sistema operativo Android.
- Gestione integrata della quarantena per l'isolamento e il trattamento di file sospetti
- Protezione Rootkit per l'individuazione di malware installati e nascosti nel sistema del computer (rootkit).
Non è disponibile per Windows XP a 64 bit
- Accesso diretto in Internet a informazioni dettagliate su virus rilevati e malware
- Aggiornamento semplice e rapido del programma, dei file delle definizioni dei virus (VDF) e del motore di ricerca tramite aggiornamento di file singolo e aggiornamento VDF incrementale mediante un server Web su Internet
- Licenza facilmente gestibile dall'utente
- Pianificatore integrato per la pianificazione di operazioni singole o ricorrenti come aggiornamenti o scansioni
- Rilevamento estremamente preciso di virus e malware per mezzo di tecnologie di scansione innovative (motore di scansione) che includono la procedura di scansione euristica
- Rilevamento di tutti i tipi di archivio convenzionali, incluso il rilevamento di archivi nascosti e Smart-Extension
- Prestazioni elevate grazie alla capacità multi threading (scansione contemporanea di molti file ad alta velocità)

2.2 Requisiti di sistema

2.2.1 Requisiti di sistema di Avira Ultimate Protection Suite

Avira Ultimate Protection Suite necessita del rispetto dei seguenti requisiti per l'uso corretto del sistema:

Sistema operativo

- Windows 8, SP più recente (a 32 o 64 bit) oppure
- Windows 7, SP più recente (a 32 o 64 bit) oppure
- Windows XP, SP più recente (a 32 o 64 bit)

Hardware

- Computer con processore Pentium o più recente, da almeno 1 GHz
- Almeno 150 MB di memoria libera sull'hard disk (maggiore quantità di memoria se si utilizza la quarantena per la memoria temporanea)
- Almeno 1024 MB RAM in Windows 8, Windows 7
- Almeno 512 MB di memoria RAM in Windows XP

Altri requisiti

- Per l'installazione del programma: diritti dell'amministratore
- Per tutte le installazioni: Windows Internet Explorer 6.0 o superiore
- Eventuale connessione Internet (vedere Prima dell'installazione)

2.2.2 Requisiti di sistema di Avira SearchFree Toolbar

I seguenti requisiti vanno rispettati al fine di garantire l'uso corretto di Avira SearchFree Toolbar:

Sistema operativo

- Windows 8, SP più recente (a 32 o 64 bit) oppure
- Windows 7, SP più recente (a 32 o 64 bit) oppure
- Windows XP, SP più recente (a 32 o 64 bit)

Web browser

- Windows Internet Explorer 6.0 o superiore
- Mozilla Firefox 3.0 o superiore
- Google Chrome 18.0 o superiore

> **Nota**
> Se necessario, disinstallare le barre di ricerca già installate prima dell'installazione di Avira SearchFree Toolbar. In caso contrario, non sarà possibile installare Avira SearchFree Toolbar.

2.2.3 Diritti di amministratore (a partire da Windows Vista)

In Windows XP molti utenti lavorano con i diritti di amministratore. Tuttavia, ciò non è auspicabile dal punto di vista della sicurezza, poiché così anche i virus e i programmi indesiderati hanno la possibilità di infiltrarsi nel computer.

Per questo motivo, Microsoft ha introdotto il controllo utente (Controllo dell'account utente). Questa funzione fa parte dei seguenti sistemi operativi:

- Windows Vista
- Windows 7
- Windows 8

Il controllo dell'account utente protegge maggiormente gli utenti registrati come amministratore, in quanto l'amministratore dispone inizialmente solo dei privilegi di un utente normale. Le azioni per le quali sono necessari diritti di amministratore sono chiaramente segnalate dal sistema operativo con un'apposita icona. Inoltre, l'utente deve esplicitamente confermare l'azione desiderata. Solo dopo aver ottenuto l'autorizzazione si registra un aumento dei privilegi e il sistema operativo esegue i propri compiti amministrativi.

Avira Ultimate Protection Suite richiede i diritti di amministratore per eseguire alcune azioni. Queste azioni sono contrassegnate dal seguente carattere: . Se questo carattere appare su un pulsante, significa che sono necessari i diritti di amministratore per eseguire l'azione. Se l'utente corrente non dispone di tali diritti, viene visualizzata una finestra di dialogo del controllo dell'account utente in cui viene richiesto di immettere la password dell'amministratore. Se non si dispone di tale password, non è possibile eseguire questa azione.

2.2.4 Incompatibilità con altri programmi

Avira Ultimate Protection Suite

Attualmente Avira Ultimate Protection Suite non è in grado di funzionare insieme ai seguenti prodotti:

- PGP Desktop Home
- PGP Desktop Professional 9.0
- CyberPatrol

Una condizione di errore nei prodotti sopraccitati può causare il non funzionamento di Avira Mail Protection (sistema di scansione POP3) di Avira Ultimate Protection Suite o l'instabilità del sistema. Avira sta collaborando con PGP e CyberPatrol per trovare una soluzione al problema. Fino ad allora si consiglia vivamente di disinstallare i prodotti sopraccitati prima dell'installazione di Avira Ultimate Protection Suite.

Avira Web Protection

Avira Web Protection non è compatibile con i seguenti prodotti:

- Teleport Pro di Tennyson Maxwell, Inc
- CHIPDRIVE® Time Recording di SCM Microsystems
- MSN Messenger di Microsoft

Pertanto i dati inviati e richiesti da tali prodotti vengono ignorati da Avira Web Protection.

> **Nota**
> Avira Mail Protection non si attiva se sullo stesso computer è già installato un server di posta elettronica (ad esempio AVM KEN, Exchange, e così via).

2.3 Licenza e aggiornamento

2.3.1 Licenza

Per poter utilizzare il prodotto Avira è necessario possedere una licenza. È necessario accettare le condizioni di licenza.

La licenza viene concessa sotto forma di codice di attivazione. Il codice di attivazione è un codice alfanumerico che l'utente riceve all'acquisto del prodotto Avira. Il codice di attivazione comprende i dati esatti della licenza, ossia quali sono i programmi dotati di licenza e per quale periodo.

Il codice viene inviato tramite e-mail se il prodotto Avira è stato acquistato su Internet, altrimenti è riportato sulla confezione del prodotto.

Per attivare la licenza del programma, è necessario immettere il codice di attivazione durante l'attivazione del programma. L'attivazione del prodotto può avvenire durante l'installazione. È però possibile attivare il prodotto Avira anche in seguito nel Sistema di gestione delle licenze in **Guida in linea > Sistema di gestione delle licenze**.

2.3.2 Estensione della licenza

Se la vostra licenza è vicina alla scadenza, Avira vi ricorda tramite una Finestra, di estenderla. Per poter far ciò, basta cliccare su un link, e verrete inoltrati al negozio online di Avira. Tuttavia, è anche possibile estendere la licenza del vostro prodotto Avira tramite il Sistema di gestione delle licenze, sotto **Guida > Sistema di gestione delle licenze**.

Se vi siete registrati nel portale delle licenze di Avira, potete anche estendere la vostra licenza tramite **Panoramica licenze** oppure selezionare l'estensione automatica.

2.3.3 Upgrade

Nel sistema di gestione delle licenze è possibile avviare l'aggiornamento di un prodotto della serie di prodotti Avira Desktop, senza bisogno di disattivare il prodotto precedente e di installare manualmente quello nuovo. Tramite l'aggiornamento dal Sistema di gestione delle licenze, immettere nell'apposito campo il codice di attivazione del prodotto di cui si desidera effettuare l'aggiornamento. Il nuovo prodotto viene installato automaticamente.

Per garantire un elevato livello di protezione e di affidabilità, Avira indica quando è disponibile un aggiornamento a una versione più recente. Fare clic su **Aggiorna** nel popup per visualizzare la pagina di aggiornamento specifica del prodotto. È possibile eseguire un aggiornamento del prodotto correntemente in uso oppure acquistare un prodotto Avira più completo. La pagina riassuntiva dei prodotti Avira mostra i prodotti attualmente utilizzati e permette di confrontarli con gli altri prodotti Avira. Per ulteriori informazioni, fare clic sull'icona Informazioni a destra accanto al nome del prodotto. Se si desidera continuare a utilizzare il prodotto in uso, fare clic su **Aggiorna** per installare subito la versione più recente con funzionalità più avanzate. Per comprare un prodotto più completo fare invece clic su **Acquista** in basso nella colonna del prodotto corrispondente. Verrà visualizzato il negozio online di Avira in cui è possibile effettuare l'ordine.

> **Nota**
> A seconda del prodotto e del sistema operativo, potrebbe essere necessario disporre di diritti di amministratore per poter eseguire l'aggiornamento. Prima di effettuare l'aggiornamento, registrarsi come amministratore.

2.3.4 Gestione delle licenze

Il sistema di gestione delle licenze di Avira Ultimate Protection Suite permette un'installazione molto semplice della licenza di Avira Ultimate Protection Suite.

Gestione delle licenze di Avira Ultimate Protection Suite

È possibile effettuare l'installazione della licenza selezionandola con un doppio clic nel Filemanager o nell'e-mail di attivazione e seguire le istruzioni delle schermate.

> **Nota**
> Il sistema di gestione delle licenze di Avira Ultimate Protection Suite copia automaticamente la licenza nella cartella del prodotto. Se è già disponibile una licenza, appare una nota che chiede se il file di licenza deve essere sostituito. In questo caso, il file preesistente viene sovrascritto dal nuovo file di licenza.

3. Installazione e disinstallazione

Questo capitolo contiene informazioni relative all'installazione di Avira Ultimate Protection Suite.

- Prima dell'installazione
- Installazione on-line da CD
- Installazione del software scaricato
- Rimozione del software incompatibile
- Selezione di un tipo di installazione
- Installazione di Avira Ultimate Protection Suite
- Modifiche all'installazione
- Disinstallazione di Avira Ultimate Protection Suite

3.1 Prima dell'installazione

✓ Prima dell'installazione verificare che il computer risponda ai Requisiti di sistema minimi.
✓ Chiudere tutte le applicazioni in esecuzione.
✓ Assicurarsi che non siano installate altre protezioni contro virus. Le funzioni automatiche di protezione di diverse applicazioni antivirus potrebbero entrare in conflitto (per le opzioni automatiche, vedere Rimozione software incompatibile).
✓ Se necessario, disinstallare le barre di ricerca già installate prima dell'installazione di Avira SearchFree Toolbar. In caso contrario, non sarà possibile installare Avira SearchFree Toolbar.
✓ Stabilire una connessione Internet.

- La connessione è necessaria per l'esecuzione dei seguenti passaggi dell'installazione:
  - Scaricare i file attuali di programma e del motore di ricerca, nonché i file di definizione dei virus aggiornati mediante il programma di installazione (per installazione basata su Internet)
  - Attivazione del programma
  - Registrazione come utente
  - Aggiornare, se necessario, a installazione conclusa

✓ Tenere a portata di mano il codice di attivazione o il file di licenza di Avira Ultimate Protection Suite se si desidera attivare il programma.
✓ Per l'attivazione o la registrazione del prodotto, Avira Ultimate Protection Suite comunica con i server Avira tramite il protocollo HTTP e la porta 80 (comunicazione Web) nonché tramite protocollo SSL e la porta 443 Se si utilizza un firewall, assicurarsi che la connessione necessaria e i dati in entrata e in uscita non vengano bloccati dal firewall.

3.2 Installazione on-line da CD

- Inserire il CD di Avira Ultimate Protection Suite.

  Se è stato abilitato l'avvio automatico, fare clic su **Apri cartella** per visualizzare i file. OPPURE

  Cercare il driver del CD, fare clic con il tasto destro su AVIRA e selezionare **Apri cartella** per visualizzare i file.

  Fare doppio clic sul file *autorun.exe*.

  Nel menu del CD, selezionare la versione on-line da installare.

  Il programma effettua una scansione per cercare i software incompatibili (maggiori informazioni qui: Rimozione del software incompatibile).

  Fare clic su **Avanti** nella schermata di *benvenuto*.

  Selezionare la lingua e fare clic su **Avanti**. Tutti i file necessari per l'installazione vengono scaricati dai server Web di Avira.

  Continuare con Selezione di un tipo di installazione.

3.3 Installazione offline da CD

- Inserire il CD di Avira Ultimate Protection Suite.

  Se è stato abilitato l'avvio automatico, fare clic su **Apri cartella** per visualizzare i file. OPPURE

  Cercare il driver del CD, fare clic con il tasto destro su AVIRA e selezionare **Apri cartella** per visualizzare i file.

  Fare doppio clic sul file *autorun.exe*.

  Nel menu del CD, selezionare la versione offline da installare.

  Il programma effettua una scansione per cercare i software incompatibili (maggiori informazioni qui: Rimozione del software incompatibile).

  Il file di installazione viene decompresso. La routine di installazione viene avviata.

  Continuare con Selezione di un tipo di installazione.

3.4 Installazione del software scaricato dal Avira Shop

- Andare su www.avira.com/download.

  Selezionare il prodotto e fare clic su **Download**.

  Salvare il file scaricato nel sistema.

  Fare doppio clic sul file di installazione avira_ultimate_protection_suite_en.exe.

  Se appare la finestra Controllo dell'account utente, fare clic su Sì

Il programma scansionerà il computer per cercare eventuali software incompatibili (maggiori informazioni qui: Rimozione del software incompatibile).

Il file di installazione viene decompresso. La routine di installazione viene avviata.

Continuare facendo clic su Selezione di un tipo di installazione.

3.5 Rimozione del software incompatibile

Il Avira Ultimate Protection Suite cerca ogni possibile software incompatibile sul vostro computer. In caso di rilevamento di software incompatibile Avira Ultimate Protection Suite genera un elenco corrispondente di questi programmi. Si consiglia di disinstallare il software che espone a rischi la sicurezza del computer.

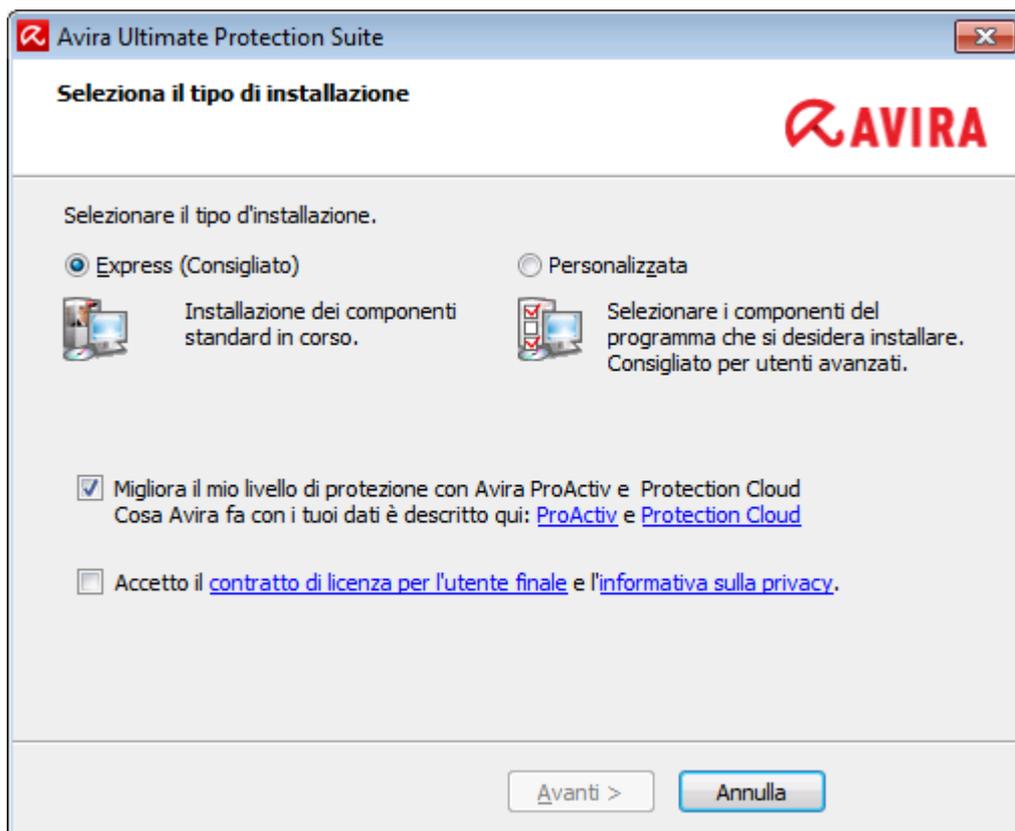
- Scegliere dall'elenco quei programmi che devono essere eliminati dal computer automaticamente, quindi fare clic su **Avanti**.

Per alcuni prodotti è necessario confermare la disinstallazione manualmente.

Selezionare i programmi e fare clic su **Avanti**.

La disinstallazione di uno o più programmi potrebbe richiedere il riavvio del computer. Dopo il riavvio, ha inizio l’installazione.

3.6 Selezione di un tipo di installazione

Durante l'installazione mediante la guida all'installazione è possibile selezionare un tipo di setup. La guida all'installazione è concepita per guidarvi con semplicità durante l'installazione.

Argomenti correlati:

- vedere Esecuzione di un'installazione express
- vedere Esecuzione di un'installazione personalizzata

3.6.1 Esecuzione di un'installazione Express

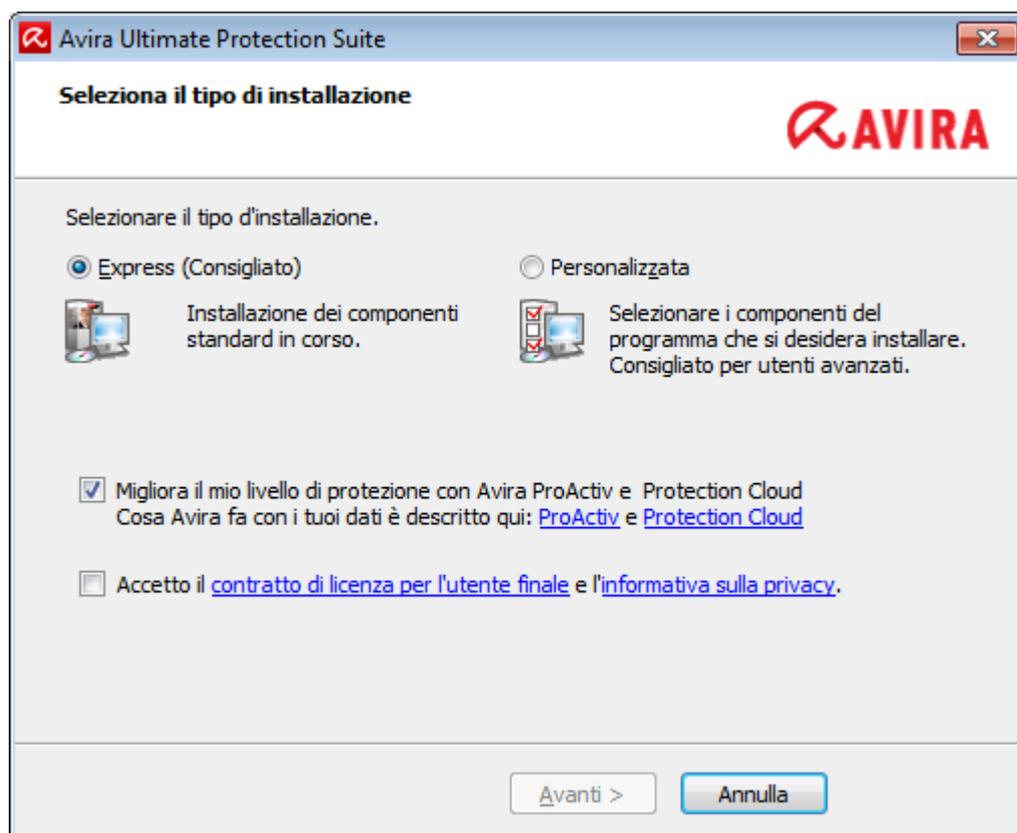
L'*installazione express* viene consigliata come configurazione di routine.

- Essa installa tutti i componenti standard di Avira Ultimate Protection Suite. Vengono utilizzate le impostazioni del livello di sicurezza consigliate da Avira.
- Uno dei seguenti percorsi viene scelto di default:
  - *C:\Program Files\Avira* (per versioni Windows 32 bit) oppure
  - *C:\Program Files (x86)\Avira* (per versioni Windows 64 bit)
- Qui sono disponibili tutti i file relativi a Avira Ultimate Protection Suite.
- Se si sceglie questo tipo di installazione, è possibile eseguire un'installazione semplicemente facendo clic su **Avanti** fino al completamento.
- Questo tipo di installazione è concepito in particolare per gli utenti non esperti in materia di configurazione di software.

3.6.2 Esecuzione di un'installazione personalizzata

La *Installazione personalizzata* permette di configurare la propria installazione. Essa è consigliata esclusivamente per utenti molto esperti in materia di hardware e software nonché di sicurezza.

- È possibile decidere di installare singoli componenti del programma.
- Si può scegliere una cartella di destinazione per i file di programma da installare.
- È possibile stabilire se **creare o meno un collegamento sul desktop e/o un gruppo di programmi sul menu di avvio**.
- Utilizzando la configurazione guidata è possibile definire le impostazioni personalizzate per Avira Ultimate Protection Suite. Inoltre, è possibile selezionare il livello di sicurezza preferito.
- Al termine dell'installazione è possibile inizializzare una scansione rapida del sistema da eseguire automaticamente dopo l'installazione.

3.7 Installazione di Avira Ultimate Protection Suite

- Se non si desidera partecipare alla Community Avira, deselezionare la casella di controllo **Desidero aumentare la mia protezione utilizzando Avira ProActiv e Protection Cloud**, preimpostata di default.

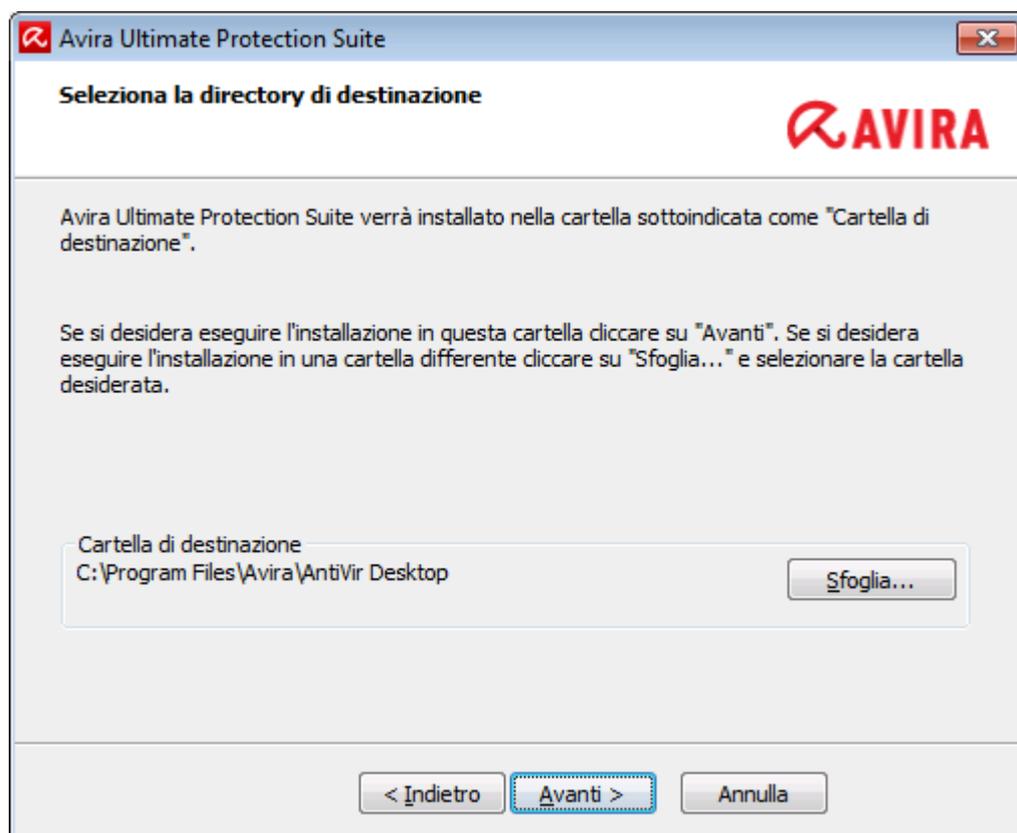
  Se si conferma la propria partecipazione alla Community Avira, Avira Ultimate Protection Suite invia a Malware Research Center Avira i dati relativi ai programmi

sospetti. I dati vengono impiegati unicamente per una più ampia verifica online e per l'ampliamento e il perfezionamento della tecnologia di rilevamento.

Facendo clic sui link **ProActiv** e **Protection Cloud** è possibile richiamare i dettagli della verifica on-line.

Confermare l'accettazione della **Contratto di licenza utente finale**. Se si desidera leggere i dettagli del **Contratto di licenza utente finale**, fare clic sul relativo link.

3.7.1 Selezione di una cartella di destinazione

L'installazione personalizzata permette di selezionare la cartella nella quale si desidera installare Avira Ultimate Protection Suite.

- Fare clic su **Sfoglia** e navigare fino alla posizione nella quale si desidera installare Avira Ultimate Protection Suite.

Selezionare la cartella nella quale si desidera installare Avira Ultimate Protection Suite nella finestra **Scegli cartella di destinazione**.

Fare clic su **Avanti**.

3.7.2 Installazione di Avira SearchFree Toolbar

Al termine del setup è possibile installare Avira SearchFree Toolbar.

Avira SearchFree Toolbar include due componenti principali: Avira SearchFree e la toolbar.

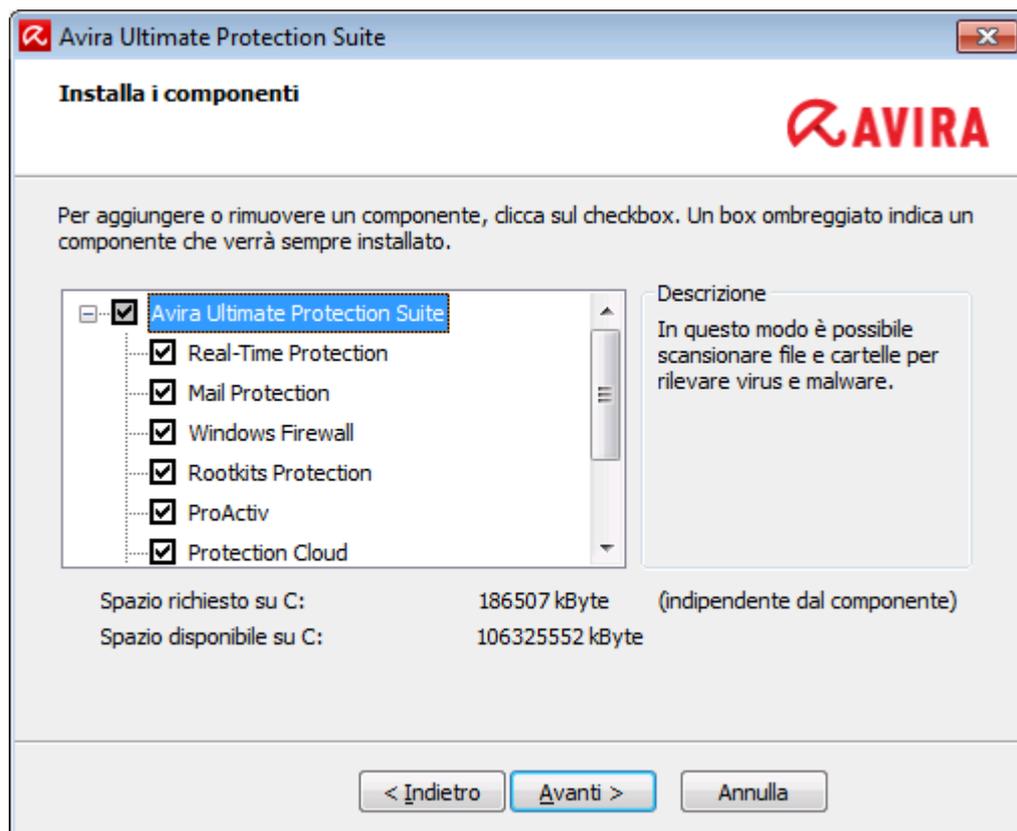
Con Avira SearchFree è possibile cercare in Internet qualsiasi numero di termini. Questo motore di ricerca visualizza tutti i risultati positivi nelle finestre del browser, valutandone il livello di sicurezza. Ciò garantisce agli utenti di Avira una navigazione più sicura in Internet.

La toolbar dispone di tre widget per le funzioni più importanti relative a Internet. È anche possibile determinare la sicurezza del sistema dell'utente attraverso il widget sicurezza del browser (solo per Firefox e Internet Explorer).

Se non si desidera installare Avira SearchFree Toolbar, deselezionare le caselle di controllo delle opzioni **Imposta come provider di ricerca predefinito** e **Imposta Avira SearchFree (avira.search.ask.com) come homepage e pagina iniziale.**

Se si rifiuta, verrà interrotta esclusivamente l'installazione di Avira SearchFree Toolbar. L'installazione di Avira Ultimate Protection Suite verrà comunque completata.

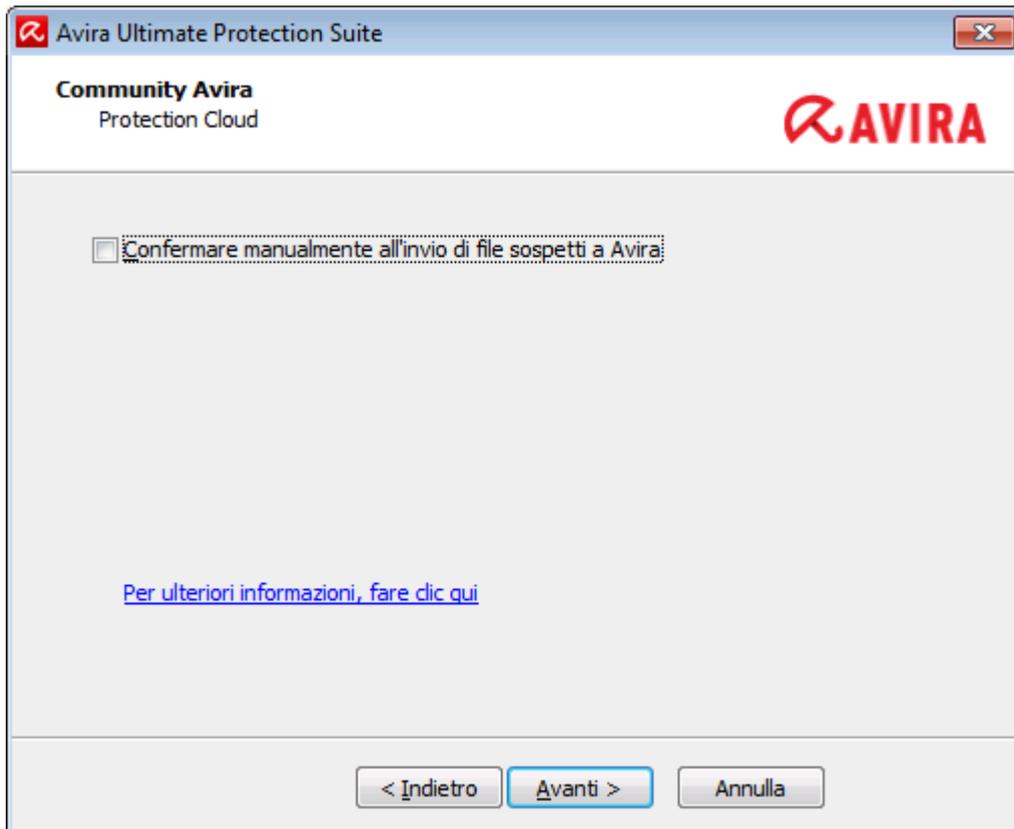
3.7.3 Selezione dei componenti di installazione

Nel caso di un'installazione personalizzata o di una modifica di un'installazione è possibile selezionare, aggiungere o eliminare i seguenti moduli.

Selezionare o deselezionare i componenti dall'elenco nel dialogo Installa componenti.

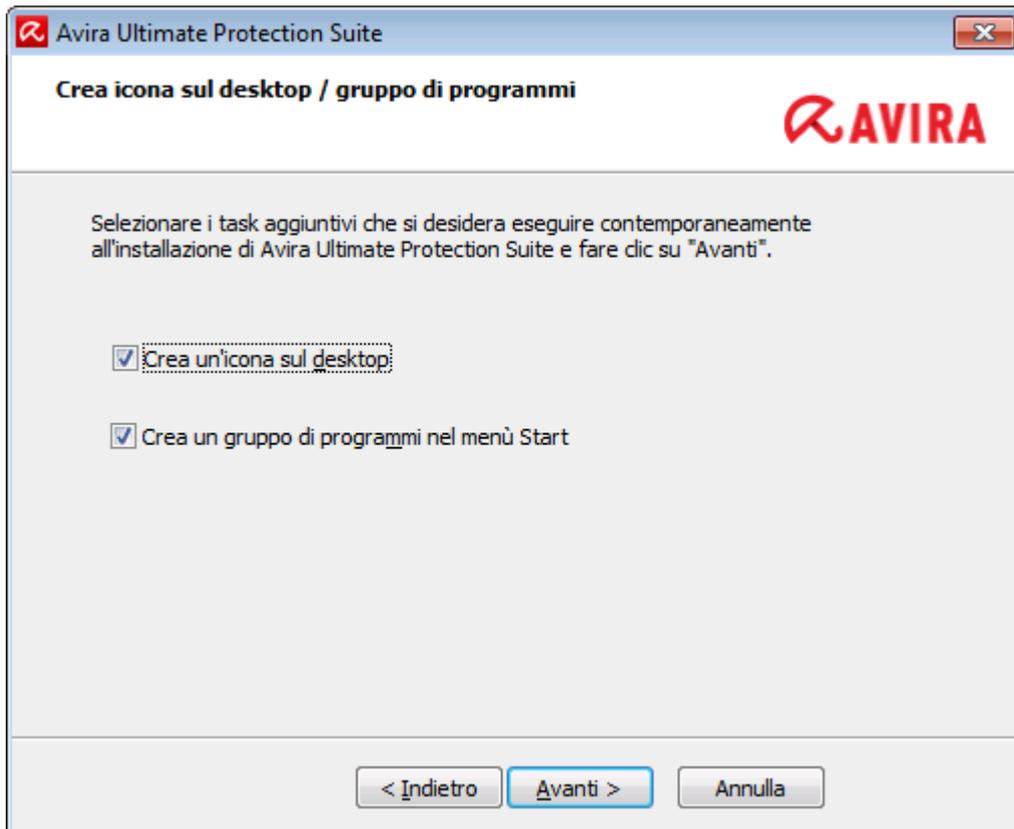
- **Avira Ultimate Protection Suite**
  Esso contiene tutti i componenti richiesti per la corretta installazione di Avira Ultimate Protection Suite.
  - **Real-Time Protection**
    Avira Real-Time Protection viene eseguito in background. Monitora e ripara i file, quando possibile, durante operazioni come apertura, scrittura e copia in tempo reale (On-Access = all'accesso). Se un utente esegue un'operazione (caricamento, esecuzione, copia di un file), Avira Ultimate Protection Suite scansiona automaticamente il file. Durante l'operazione di rinomina del file, Avira Real-Time Protection non esegue alcuna scansione.
  - **Mail Protection**
    Mail Protection è l'interfaccia fra il computer e il server e-mail da cui il programma di e-mail (Email-Client) scarica le e-mail. Mail Protection funge da cosiddetto proxy tra il programma e-mail e il server e-mail. Tutte le e-mail in entrata vengono convogliate mediante questo proxy, e, una volta ricercati virus e programmi indesiderati, vengono inoltrate al programma di e-mail. In base alla configurazione, il programma tratta le e-mail infette automaticamente o chiede all'utente l'azione da eseguire.
  - **Windows Firewall** (a partire da Windows 7)
    Questo componente gestisce il Windows Firewall di Avira Ultimate Protection Suite.
  - **Rootkits Protection**
    Avira Rootkits Protection controlla se sul computer sono già installati software che dopo l'intrusione nel computer non si riesce a rilevare con i metodi convenzionali del riconoscimento di malware.

- **ProActiv**
  Il componente ProActiv monitora le azioni dell'applicazione e avvisa gli utenti circa i comportamenti dell'applicazione sospetti. Grazie a questo riconoscimento basato sul comportamento è possibile proteggersi dai malware. Il componente ProActiv è integrato in Avira Real-Time Protection.
- **Protection Cloud**
  Il componente Protection Cloud è un modulo per il rilevamento on-line dinamico di malware ancora sconosciuti. Ciò significa che i file vengono caricati in una posizione remota e confrontati con file conosciuti nonché altri file in fase di caricamento e vengono analizzati in tempo reale (senza programmazione e ritardo). In questo modo il database viene costantemente aggiornato, pertanto è possibile garantire un livello di sicurezza ancora maggiore.
  Se è stato selezionato il componente Protection Cloud ma si desidera comunque confermare sempre manualmente quali file caricare per l'analisi del cloud, selezionare l'opzione **Confermare manualmente all'invio di file sospetti a Avira**.
- **Web Protection**
  Quando si naviga su Internet, mediante il browser Web i dati vengono recuperati da un server Web. I dati trasferiti dal server Web (file HTML, file di script e immagini, file flash, file audio e video, ecc.) normalmente passano dalla cache del browser direttamente all'esecuzione nel browser Web cosicché non è possibile una scansione in tempo reale così come messa a disposizione da Avira Real-Time Protection. In questo modo virus e programmi indesiderati potrebbero entrare nel computer. Web Protection è un cosiddetto proxy HTTP che monitora le porte utilizzate per il trasferimento dei dati (80, 8080, 3128) e controlla la presenza di virus e programmi indesiderati nei file trasferiti. In base alla configurazione, il programma tratta i file infetti automaticamente o chiede all'utente l'azione da eseguire.
- **Estensione shell**
  Le estensioni Shell creano nel menu contestuale di Esplora risorse di Windows (tasto destro del mouse) la voce **Controlla i file selezionati con Avira**. Con questa voce è possibile scansionare direttamente singoli file o directory.

Argomenti correlati:
Modifiche a un'installazione

Se hai deciso di partecipare alla Community Avira, puoi scegliere ogni volta di confermare manualmente il caricamento del file che deve essere inviato a Avira Malware Research Center.

- Per Avira Ultimate Protection Suite, per chiedere conferma ogni volta, attivare l'opzione **Conferma manualmente quando invii dei file sospetti a Avira**.

3.7.4 Creazione di collegamenti per Avira Ultimate Protection Suite

È possibile accedere a Avira Ultimate Protection Suite in modo più rapido e semplice grazie a un'icona sul desktop e/o a un gruppo di programmi nel menu di avvio.

- Per creare un collegamento sul desktop per Avira Ultimate Protection Suite e/o un gruppo di programmi nel **menu Avvio**, lasciare attive le opzioni.

3.7.5 Attivazione di Avira Ultimate Protection Suite

Vi sono modi diversi per attivare Avira Ultimate Protection Suite.

Se si dispone già di un codice di attivazione, inserirlo negli appositi campi.

- Se non si dispone ancora di un codice di attivazione, fare clic sul link Acquista un codice di attivazione.

  Si verrà indirizzati al sito Web di Avira, dove sarà possibile acquistare un codice di attivazione.

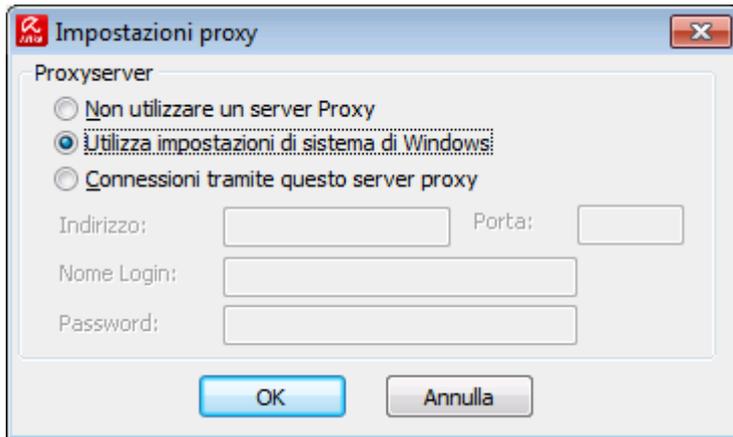
- Se si desidera solamente provare il prodotto, selezionare **Prova prodotto** e inserire i propri dati nei campi di registrazione richiesti.

  La licenza di prova ha una validità di 31 giorni.

- Se è già stato attivato un prodotto e si desidera reinstallare il proprio prodotto Avira, selezionare l'opzione **Ho già un file di licenza valido**.

  Si aprirà una finestra del browser e sarà possibile cercare il file *hbedv.key* nel vostro sistema.

3.7.6 Definizione delle impostazioni proxy

La definizione delle impostazioni proxy è consigliata esclusivamente per utenti molto esperti in materia di hardware e software nonché di sicurezza.

- Qualora non sia previsto che Avira Ultimate Protection Suite si connetta a Internet via server proxy, attivare l'opzione **Non utilizzare un server proxy**.
- Se si desidera che Avira Ultimate Protection Suite si connetta a Internet come le altre applicazioni installate, lasciare abilitata l'opzione **Utilizza impostazioni di sistema di Windows** (attivata di default).

  Accedendo a **Pannello di controllo > Opzioni Internet > Connessioni > Impostazioni LAN** è possibile configurare le impostazioni di sistema di Windows in modo tale che venga utilizzato un server proxy. Per accedere a Opzioni Internet è possibile utilizzare anche il menu **Strumenti** di Internet Explorer.

Nota
Se si utilizza un server proxy che richiede l'autenticazione, specificare tutti i dati richiesti in **Connessioni via questo server proxy**. L'opzione **Utilizza impostazioni di sistema di Windows** può essere selezionata solo in presenza di server proxy che non richiedono alcuna autenticazione.

- Per impostare un server proxy associato in modo specifico a Avira Ultimate Protection Suite, attivare **Connessioni tramite questo server proxy** e inserire le relative informazioni:

Indirizzo

Inserire il nome del computer o l'indirizzo IP del server proxy che si desidera utilizzare per la connessione al server Web.

Esempi:

Indirizzo: proxy.dominio.it

Indirizzo: 192.168.1.100

Porta

Inserire il numero della porta del server proxy che si desidera utilizzare per la connessione al server Web.

Esempi:

Porta: 8080

Porta: 3128

Nome login

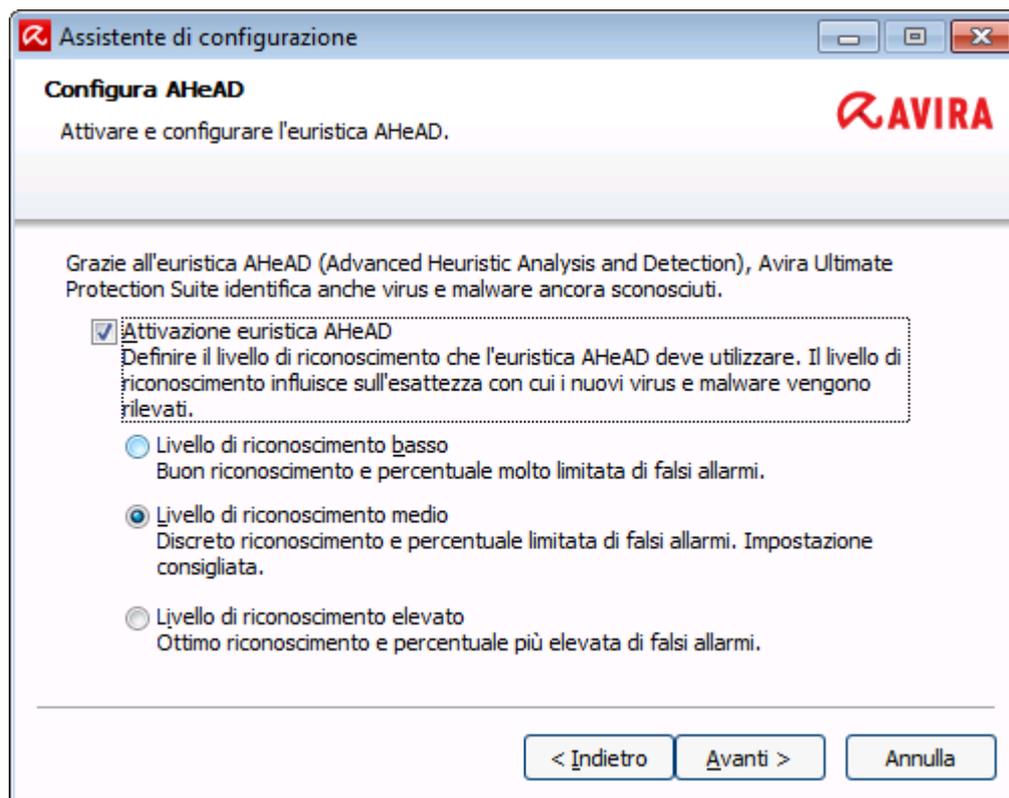
Inserire un nome utente per il login al server proxy.

Password login

Inserire la password appropriata per il login al server proxy. La password è memorizzata criptata. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*).

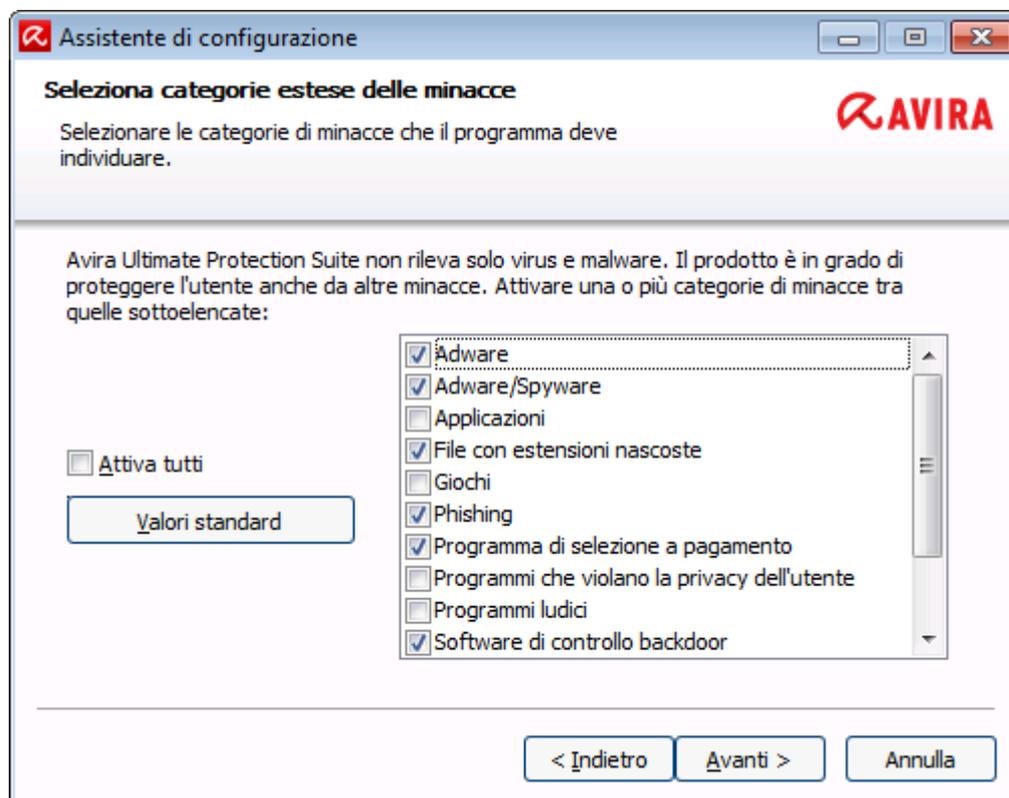
Fare clic su **OK**.

3.7.7 Configurazione del livello di rilevamento euristico (AHeAD)

Avira Ultimate Protection Suite contiene, grazie alla tecnologia AHeAD di Avira (*Advanced Heuristic Analysis and Detection*), un tool molto efficace. Questa tecnologia utilizza tecniche di riconoscimento di pattern in grado di rilevare malware sconosciuti (nuovi) grazie alla precedente analisi di altri malware.

- Selezionare un livello di rilevamento nella finestra di dialogo **Configura AHeAD** e fare clic su **Avanti**.

  Il livello di rilevamento selezionato viene registrato per l'impostazione della tecnologia AHeAD di System Scanner (scansione diretta) e di Real-Time Protection (scansione in tempo reale).

3.7.8 Selezione delle categorie estese delle minacce

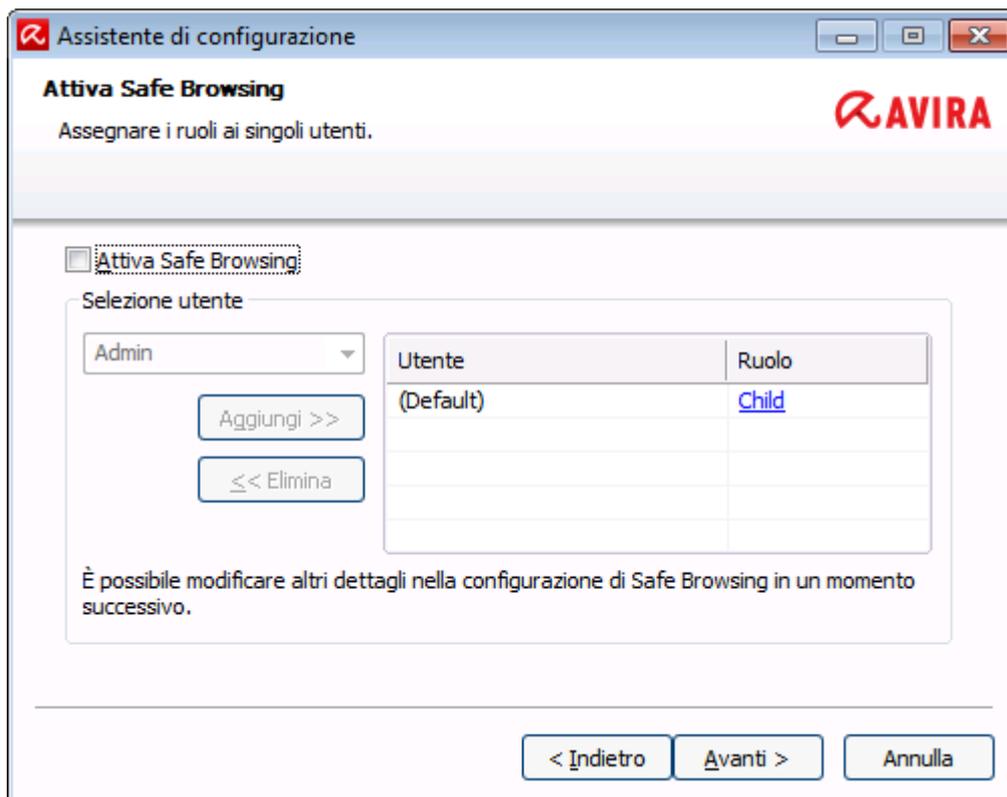
Virus e malware non sono le uniche minacce che costituiscono un pericolo per il sistema del computer. È stato definito un elenco completo di rischi, classificati in categorie di minacce estese.

- Alcune categorie di minacce sono già state selezionate di default.

  Se necessario, attivare ulteriori categorie delle minacce nella finestra di dialogo **Selezione delle categorie estese delle minacce**.

  Qualora si cambi idea, è possibile tornare indietro ai valori consigliati facendo clic sul pulsante **Valori di default**.

  Continuare l'installazione facendo clic su **Avanti**.

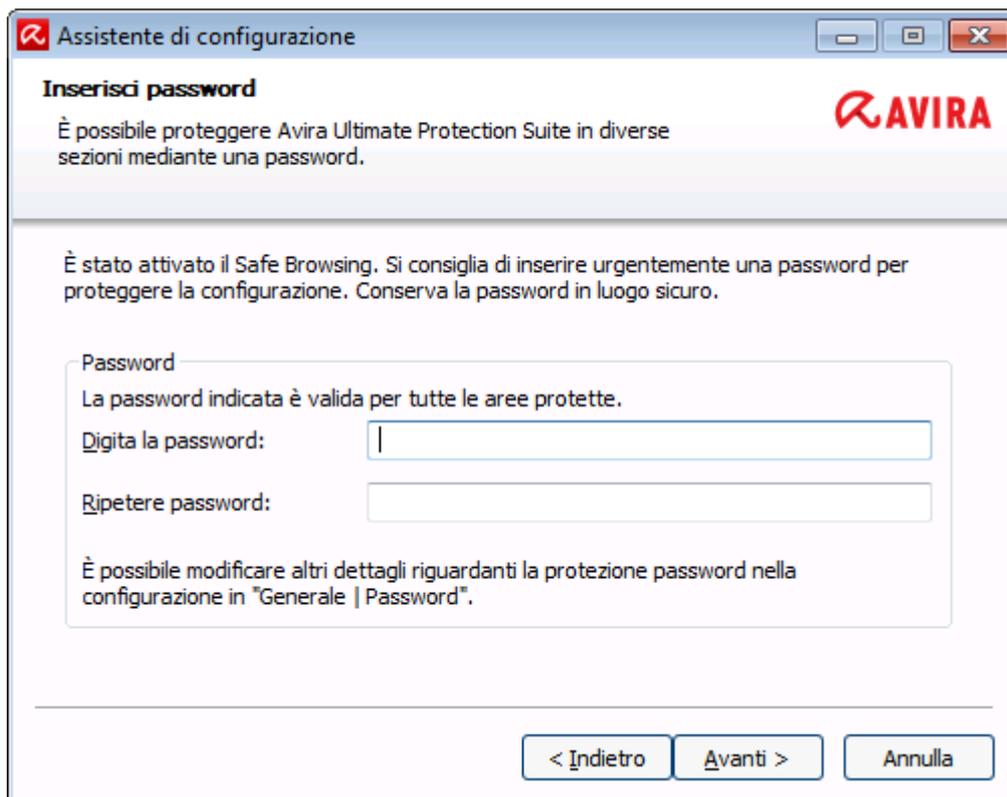
3.7.9 Attivazione di Safe Browsing

Il programma Avira in uso è provvisto della funzione **Safe Browsing** per filtrare offerte Internet indesiderate o illegali e per la limitazione temporale dell'utilizzo di Internet. La funzione **Safe Browsing** fa parte del componente *PROTEZIONE DEI BAMBINI*.

- Se è stato selezionato il modulo Web Protection è possibile:

- Assegnare i ruoli **Bambino**, **Ragazzo** o **Adulto** agli utenti del computer per l'utilizzo di Internet
- Disabilitare Safe Browsing nella finestra di dialogo **Abilita Safe Browsing**

Fare clic su **Avanti**.

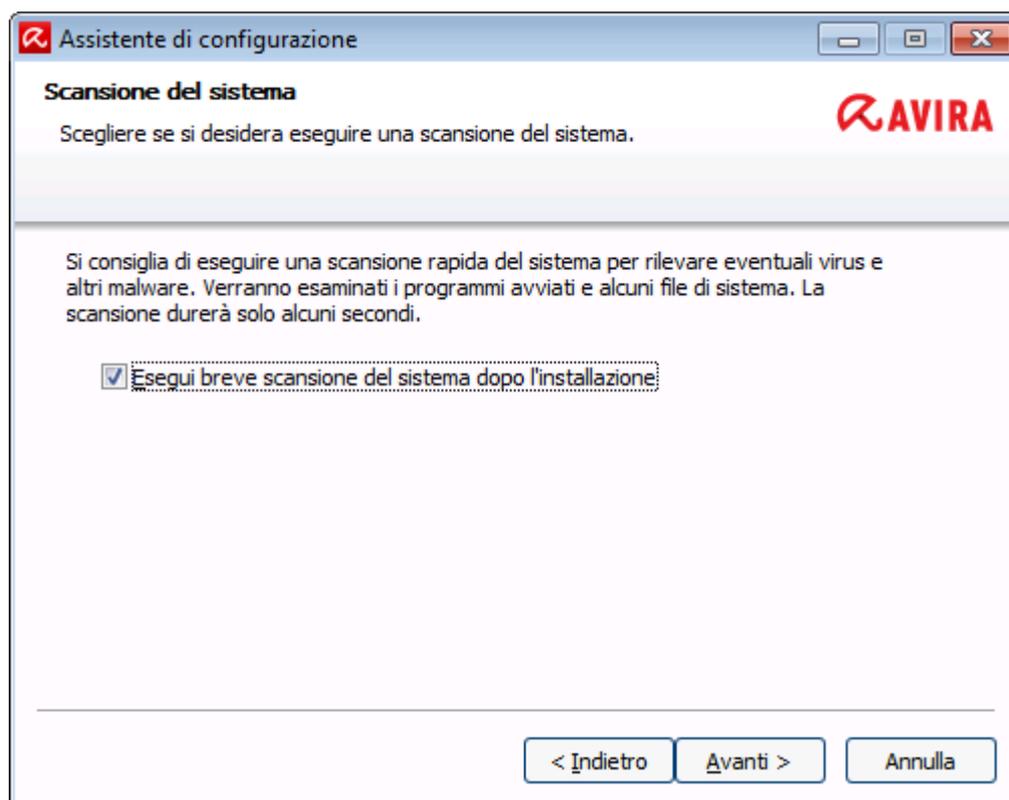
3.7.10 Assegnazione di una password

Se è stato abilitato Safe Browsing, è possibile impostare una password per proteggere le impostazioni di configurazione da modifiche da parte dei vostri figli o di un altro utente del computer.

- Inserire una password nella finestra di dialogo.

  Ripetere la password.

  Fare clic su **Avanti**.

3.7.11 Avvio di una scansione dopo l'installazione

Per verificare lo stato di sicurezza corrente del computer, è possibile eseguire una scansione rapida del sistema una volta completata la configurazione e prima che il computer venga riavviato. System Scanner scansiona i programmi in esecuzione e i file di sistema più importanti alla ricerca di virus e malware.

- Se si desidera eseguire una scansione rapida del sistema, lasciare attivata l'opzione **Scansione rapida del sistema**.

  Fare clic su **Avanti**.

  Completare la configurazione facendo clic su **Fine**.

  Se non è stata disattivata l'opzione **Scansione rapida del sistema**, si apre la finestra *Luke Filewalker*.

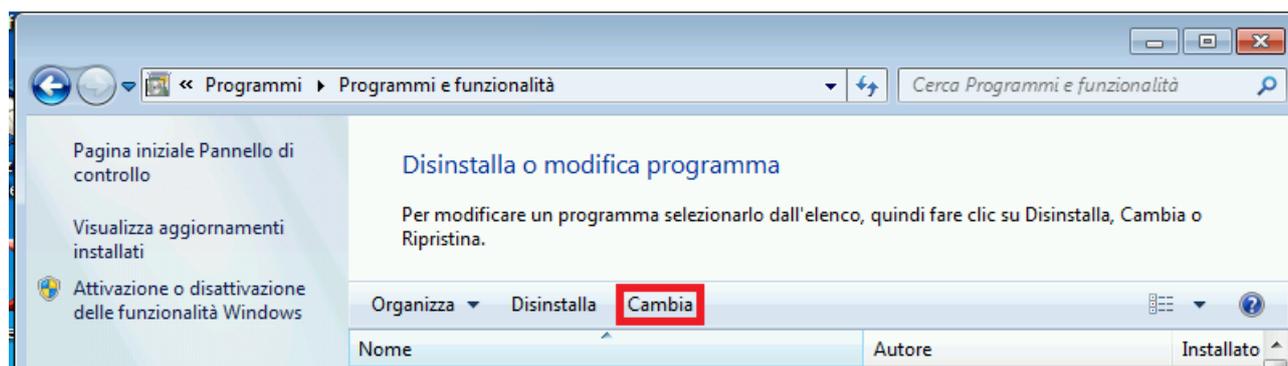
  System Scanner esegue una scansione rapida del sistema.

3.8 Modifiche all'installazione

Se si desidera aggiungere o eliminare moduli del programma dell'installazione corrente, non è necessario disinstallare Avira Ultimate Protection Suite. La procedura è la seguente:

- Modifica a un'installazione in Windows 8
- Modifica a un'installazione in Windows 7
- Modifica a un'installazione in Windows XP

3.8.1 Modifica a un'installazione in Windows 8

È possibile aggiungere o rimuovere singoli componenti del programma all'attuale installazione del Avira Ultimate Protection Suite (vedere Selezione dei componenti di installazione).

Se si desidera aggiungere o eliminare componenti del programma dell'installazione corrente, è possibile utilizzare l'opzione **Disinstalla programmi** nel **Pannello di controllo di Windows** per **Modificare/Disinstallare** programmi.

- Fare clic con il tasto destro sullo schermo.

  Apparirà il simbolo **Tutte le app**.

  Fare clic sul simbolo e cercare il **Pannello di controllo** nella sezione *App - Sistema Windows*.

  Fare doppio clic sul simbolo del **Pannello di controllo**.

  Fare clic su **Programmi - Disinstalla un programma**.

  Fare clic su **Programmi e funzionalità - Disinstalla un programma**.

  Selezionare Avira Ultimate Protection Suite e fare clic su **Cambia**.

  Nella finestra di dialogo di **benvenuto**del programma, selezionare l'opzione **Modifica**. Si è così inseriti nella modifica dell'installazione.

Argomenti correlati:
Selezione dei componenti di installazione

3.8.2 Modifica a un'installazione in Windows 7

È possibile aggiungere o rimuovere singoli componenti del programma all'attuale installazione del Avira Ultimate Protection Suite (vedere Selezione dei componenti di installazione).

Se si desidera aggiungere o eliminare componenti del programma dell'installazione corrente, è possibile utilizzare l'opzione **Installazione applicazioni**, **Cambia/Rimuovi programmi** all'interno del **Pannello di controllo** di Windows.

- Aprire nel menu **Start** di Windows il **Pannello di controllo**.

  Fare doppio clic su **Programmi e funzionalità**.

  Selezionare Avira Ultimate Protection Suite e fare clic su **Cambia**.

  Nella finestra di dialogo di **benvenuto**del programma, selezionare l'opzione **Modifica**. Si è così inseriti nella modifica dell'installazione.

Argomenti correlati:
Selezione dei componenti di installazione

3.8.3 Modifica a un'installazione in Windows XP

È possibile aggiungere o rimuovere singoli componenti del programma all'installazione del Avira Ultimate Protection Suite (vedere Selezione dei moduli di installazione).

Se si desidera aggiungere o eliminare componenti del programma dell'installazione corrente, è possibile utilizzare l'opzione **Installazione applicazioni**, **Cambia/Rimuovi programmi** all'interno del **Pannello di controllo** di Windows.

- Aprire nel menu **Start > Impostazioni** di Windows il **Pannello di controllo**.

  Fare doppio clic su **Aggiungi o rimuovi programmi**.

  Selezionare Avira Ultimate Protection Suite e fare clic su **Cambia**.

  Nella finestra di dialogo di **benvenuto**del programma, selezionare l'opzione **Modifica**. Si è così inseriti nella modifica dell'installazione.

Argomenti correlati:
Selezione dei componenti di installazione

3.9 Disinstallazione di Avira Ultimate Protection Suite

Qualora si desideri disinstallare Avira Ultimate Protection Suite, la procedura è la seguente:

- Disinstallazione di Avira Ultimate Protection Suite in Windows 8
- Disinstallazione di Avira Ultimate Protection Suite in Windows 7
- Disinstallazione di Avira Ultimate Protection Suite in Windows XP

3.9.1 Disinstallazione di Avira Ultimate Protection Suite in Windows 8

Per disinstallare il prodotto Avira Ultimate Protection Suite dal proprio computer, utilizzare l'opzione **Programmi e funzionalità** nel Pannello di controllo di Windows.

- Fare clic con il tasto destro sullo schermo.

  Apparirà il simbolo **Tutte le app**.

  Fare clic sul simbolo e cercare il **Pannello di controllo** nella sezione *App - Sistema Windows*.

  Fare doppio clic sul simbolo del **Pannello di controllo**.

  Fare clic su **Programmi - Disinstalla un programma**.

  Fare clic su **Programmi e funzionalità - Disinstalla un programma**.

  Selezionare Avira Ultimate Protection Suite nell'elenco e fare clic su **Disinstalla**.

  Alla domanda se si desideri davvero rimuovere l'applicazione e i suoi componenti, fare clic su **Sì** per confermare.

  Alla domanda se si desideri attivare Windows Firewall (Avira FireWall verrà disinstallato), fare clic su **Sì** per confermare e mantenere la protezione per il sistema.

  Tutti i componenti del programma vengono eliminati.

  Fare clic su **Fine** per terminare la disinstallazione.

  Qualora appaia una finestra di dialogo con il suggerimento di riavviare il computer, fare clic su **Sì** per confermare.

  Avira Ultimate Protection Suite viene quindi disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro del programma vengono eliminate.

> **Nota**
> Avira SearchFree Toolbar non è compresa nel programma di disinstallazione e deve essere disinstallata separatamente.

3.9.2 Disinstallazione di Avira Ultimate Protection Suite in Windows 7

Per disinstallare il prodotto Avira Ultimate Protection Suite dal proprio computer, utilizzare l'opzione **Programmi e funzionalità** nel Pannello di controllo di Windows.

- Aprire nel menu **Start** di Windows il **Pannello di controllo**.

  Fare doppio clic su **Programmi e funzionalità**.

  Selezionare Avira Ultimate Protection Suite nell'elenco e fare clic su **Disinstalla**.

  Alla domanda se si desideri davvero rimuovere l'applicazione e i suoi componenti, fare clic su **Sì** per confermare.

  Alla domanda se si desideri attivare Windows Firewall (Avira FireWall verrà disinstallato), fare clic su **Sì** per confermare e mantenere la protezione per il sistema.

  Tutti i componenti del programma vengono eliminati.

  Fare clic su **Fine** per terminare la disinstallazione.

  Qualora appaia una finestra di dialogo con il suggerimento di riavviare il computer, fare clic su **Sì** per confermare.

  Avira Ultimate Protection Suite viene quindi disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro del programma vengono eliminate.

Nota
Avira SearchFree Toolbar non è compresa nel programma di disinstallazione e deve essere disinstallata separatamente.

3.9.3 Disinstallazione di Avira Ultimate Protection Suite in Windows XP

Per disinstallare Avira Ultimate Protection Suite dal proprio computer, utilizzare l'opzione **Cambia/Rimuovi programmi** nel Pannello di controllo di Windows.

- Aprire nel menu **Start > Impostazioni** di Windows il **Pannello di controllo**.

  Fare doppio clic su **Aggiungi o rimuovi programmi**.

  Selezionare Avira Ultimate Protection Suite nell'elenco e fare clic su **Rimuovi**.

  Alla domanda se si desideri davvero rimuovere l'applicazione e i suoi componenti, fare clic su **Sì** per confermare.

  Tutti i componenti del programma vengono eliminati.

Fare clic su **Fine** per terminare la disinstallazione.

Qualora appaia una finestra di dialogo con il suggerimento di riavviare il computer, fare clic su **Sì** per confermare.

Avira Ultimate Protection Suite viene quindi disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro del programma vengono eliminate.

> **Nota**
> Avira SearchFree Toolbar non è compresa nel programma di disinstallazione e deve essere disinstallata separatamente.

3.9.4 Disinstallazione di Avira SearchFree Toolbar

Qualora si desideri disinstallare Avira SearchFree Toolbar, la procedura è la seguente:

- Disinstallazione di Avira SearchFree Toolbar in Windows 8
- Disinstallazione di Avira SearchFree Toolbar in Windows 7
- Disinstallazione di Avira SearchFree Toolbar in Windows XP
- Disinstallazione di Avira SearchFree Toolbar mediante il browser Web
- Disinstallazione Avira SearchFree Toolbar mediante Gestione Add-Ons

Disinstallazione di Avira SearchFree Toolbar in Windows 8

Per disinstallare Avira SearchFree Toolbar:

- Chiudere il browser Web.

Fare clic con il tasto destro su uno degli angoli inferiori dello schermo.

Apparirà il simbolo **Tutte le app**.

Fare clic sul simbolo e cercare il **Pannello di controllo** nella sezione *App - Sistema Windows*.

Fare doppio clic sul simbolo del **Pannello di controllo**.

Fare clic su **Programmi - Disinstalla un programma**.

Fare clic su **Programmi e funzionalità - Disinstalla un programma**.

Selezionare Avira SearchFree Toolbar plus Web Protection nell'elenco e fare clic su **Disinstalla**.

Verrà chiesto all'utente se desidera davvero disinstallare il prodotto.

Confermare con **Sì**.

Avira SearchFree Toolbar plus Web Protection viene disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro di Avira SearchFree Toolbar plus Web Protection vengono eliminate.

Disinstallazione di Avira SearchFree Toolbar in Windows 7

Per disinstallare Avira SearchFree Toolbar:

- Chiudere il browser Web.

  Aprire nel menu **Start** di Windows il **Pannello di controllo**.

  Fare doppio clic su **Programmi e funzionalità**.

  Selezionare Avira SearchFree Toolbar plus Web Protection nell'elenco e fare clic su **Disinstalla**.

  Verrà chiesto all'utente se desidera davvero disinstallare il prodotto.

  Confermare con **Sì**.

  Avira SearchFree Toolbar plus Web Protection viene disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro di Avira SearchFree Toolbar plus Web Protection vengono eliminate.

Disinstallazione di Avira SearchFree Toolbar in Windows XP

Per disinstallare Avira SearchFree Toolbar:

- Chiudere il browser Web.

  Aprire nel menu **Start > Impostazioni** di Windows il **Pannello di controllo**.

  Fare doppio clic su **Aggiungi o rimuovi programmi**.

  Selezionare Avira SearchFree Toolbar plus Web Protection nell'elenco e fare clic su **Rimuovi**.

  Verrà chiesto all'utente se desidera davvero disinstallare il prodotto.

  Confermare con **Sì**.

  Avira SearchFree Toolbar plus Web Protection viene disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro di Avira SearchFree Toolbar plus Web Protection vengono eliminate.

Disinstallazione di Avira SearchFree Toolbar mediante il browser Web

È inoltre possibile disinstallare Avira SearchFree Toolbar in Firefox e Internet Explorer direttamente dal browser.

- Aprire il browser Web.

  Nella barra di ricerca aprire il menu **Opzioni**.

  Fare clic su **Disinstalla barra degli strumenti dal browser**.

  Alla domanda se si desideri installare il prodotto, fare clic su **Sì** per confermare.

  Ora verrà chiesto di chiudere il browser Web.

  Chiudere il browser Web e fare clic su **Riprova**.

Avira SearchFree Toolbar plus Web Protection viene disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro di Avira SearchFree Toolbar plus Web Protection vengono eliminate.

> **Nota**
> Per disinstallare l'Avira SearchFree Toolbar, è necessario abilitare la toolbar in Gestione Add-ons.

Disinstallazione di Avira SearchFree Toolbar mediante Gestione Add-ons

Poiché la toolbar è installata come Add-On, è anche possibile gestire il tool con differenti manager di Add-On.

Firefox

- Fare clic su **Strumenti > Add-ons > Estensioni**. Qui è possibile gestire l'Add-on Avira, ossia attivare e disattivare o disinstallare la toolbar.

Internet Explorer

- Fare clic su **Gestione Add-ons > Barra degli strumenti ed Estensioni**. Qui è possibile attivare e disattivare o disinstallare Avira SearchFree Toolbar.

Google Chrome

- Fare clic su **Opzioni > Estensioni** per gestire in modo semplice la toolbar, ossia per attivarla, disattivarla o disinstallarla.

4. Panoramica di Avira Ultimate Protection Suite

In questo capitolo è possibile consultare una panoramica delle funzionalità e del funzionamento del prodotto Avira.

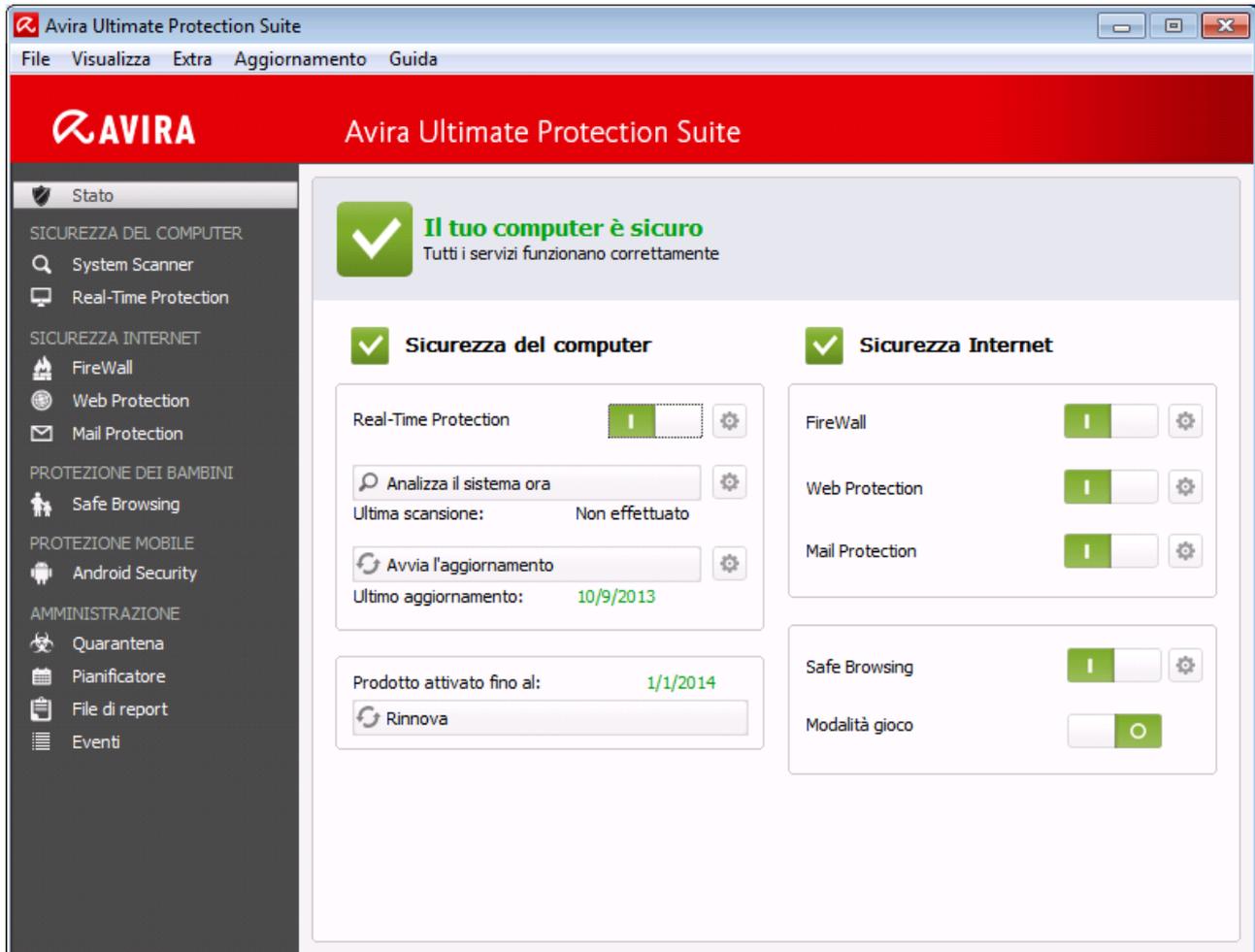
- vedere capitolo Interfaccia utente e funzionamento
- vedere capitolo Avira SearchFree Toolbar
- vedere capitolo Come procedere

4.1 Interfaccia utente e funzionamento

È possibile usare il prodotto Avira mediante tre elementi dell'interfaccia del programma:

- Control Center: monitoraggio e gestione del prodotto Avira
- Configurazione: configurazione del prodotto Avira
- Icona Tray nella barra delle applicazioni: apertura di Control Center e altre funzioni

4.1.1 Control Center

Control Center serve per il monitoraggio dello stato di protezione del computer e per la gestione e il funzionamento dei componenti di protezione e delle funzioni del prodotto Avira in uso.

La finestra di Control Center è suddivisa in tre aree: la **barra dei menu**, l' **area di navigazione** e la finestra dettagliata **Stato**:

- **Barra dei menu:** nei menu di Control Center è possibile richiamare funzioni generali del programma e informazioni sul prodotto.
- **Area di navigazione:** nell'area di navigazione è possibile passare in modo semplice da una rubrica all'altra di Control Center. Le singole rubriche contengono informazioni e funzioni dei componenti del programma e sono presenti sulla barra di navigazione in base alle sezioni dei task. Esempio: sezione dei task *SICUREZZA DEL COMPUTER* - Rubrica **Real-Time Protection**.
- **Stato:** nella schermata iniziale **Stato** viene mostrato se il computer è sufficientemente protetto, quali moduli sono attivi e quando sono stati eseguiti l'ultimo backup e l'ultima scansione del sistema. Nella finestra **Stato** sono presenti i pulsanti per l'esecuzione di funzioni e operazioni, ad esempio l'attivazione o disattivazione di **Real-Time Protection**.

Avvio e chiusura di Control Center

Per avviare Control Center è possibile scegliere tra le seguenti modalità:

- Fare doppio clic sull'icona del programma sul desktop

- Mediante la voce del programma nel menu **Start > Programmi**.
- Mediante l'icona della barra delle applicazioni del prodotto Avira.

Si può chiudere Control Center mediante il comando **Chiudi** nel menu **File**, con la combinazione di tasti **Alt+F4** o facendo clic sulla x nella finestra di Control Center.

Utilizzo di Control Center

Come navigare in Control Center:

- Fare clic sulla barra di navigazione su un'area del task sotto la rubrica.
  - ↳ La sezione dei task viene visualizzata con ulteriori possibilità di funzione e di configurazione nella finestra dettagliata.
- Eventualmente fare clic su un'altra sezione dei task per visualizzarla nella finestra dettagliata.

> **Nota**
> Attivare la navigazione da tastiera nella barra dei menu con l'ausilio del tasto [**Alt**]. Con il tasto **Invio** si attiva la voce di menu selezionata in quel momento. Per aprire, chiudere o navigare nei menu di Control Center è possibile utilizzare anche le combinazioni di tasti [**Alt**] + carattere sottolineato nel menu o comando. Tenere premuto il tasto [**Alt**] se si desidera richiamare dal menu un comando o un sottomenu.

Come elaborare dati o oggetti che vengono visualizzati nella finestra dei dettagli:

- Evidenziare i dati o gli oggetti che si desidera elaborare.

  Per evidenziare più elementi, tenere premuto il tasto **Ctrl** o il tasto **Maiusc** (selezione di elementi consecutivi) durante la selezione degli elementi.
- Fare clic sui pulsanti desiderati nella barra superiore della finestra dei dettagli per elaborare l'oggetto.

Control Center in sintesi

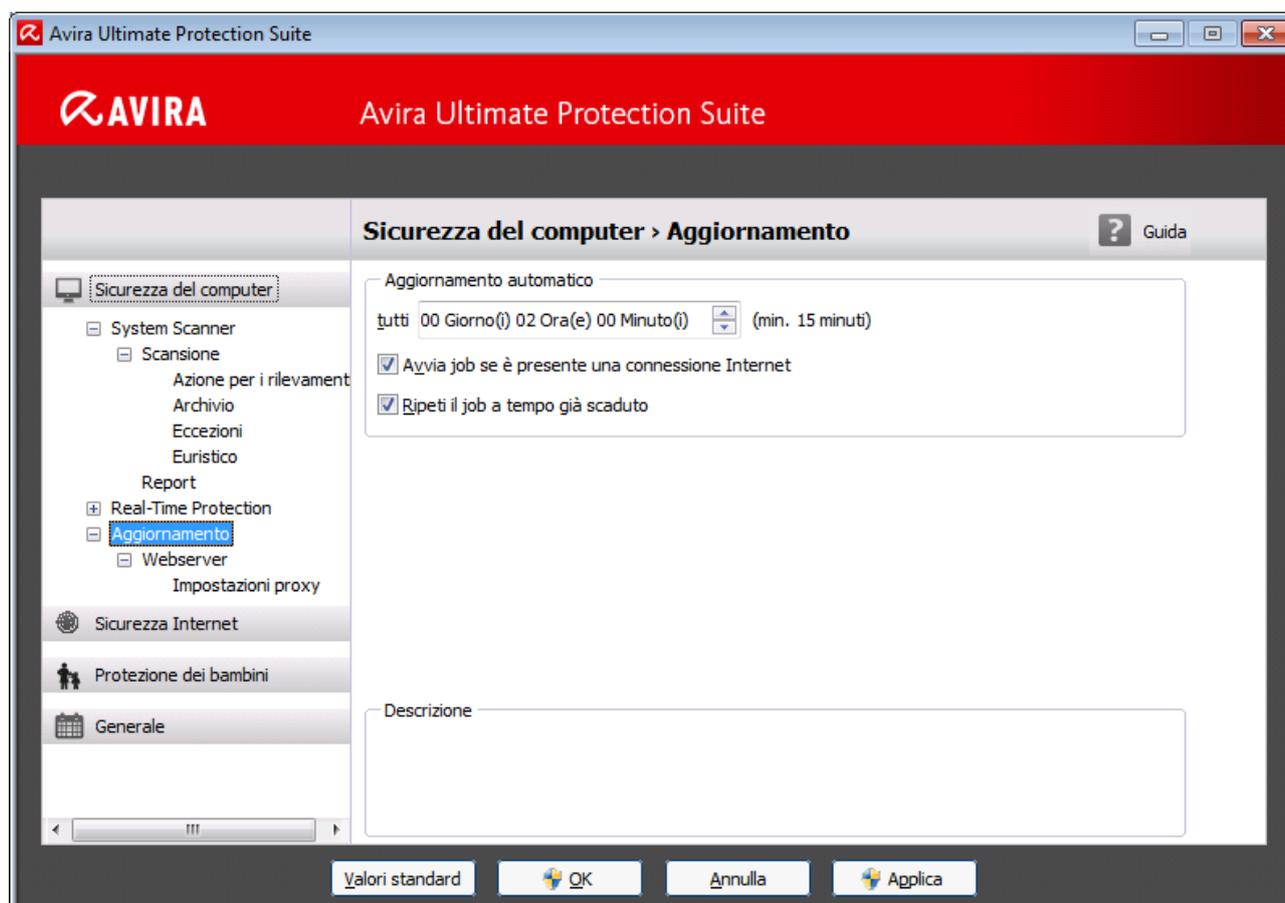
- **Stato**: nella schermata iniziale **Stato** sono presenti tutte le rubriche per controllare le funzionalità del programma (vedere Stato).
  - La finestra **Stato** offre la possibilità di visualizzare quali moduli sono attivi e fornisce informazioni sull'ultimo aggiornamento effettuato.
- *SICUREZZA DEL COMPUTER*: in questa rubrica sono disponibili i componenti con cui eseguire la scansione di virus e malware nei file del computer.
  - La rubrica **System Scanner** offre la possibilità di configurare o avviare la scansione diretta in modo semplice (vedere System Scanner). I profili predefiniti consentono di eseguire una scansione con le opzioni standard già adeguate. Con l'aiuto della Selezione manuale (viene memorizzata) o con la creazione di Profili personalizzati, è

possibile adattare la scansione di virus e programmi indesiderati alle proprie esigenze personali.

- La rubrica Real-Time Protection mostra le informazioni sui file scansionati e altri dati statistici, che possono essere ripristinati in ogni momento e permette di richiamare il file di report. Informazioni dettagliate sull'ultimo virus o programma indesiderato trovato sono reperibili premendo un pulsante.

- *SICUREZZA INTERNET*: contiene i componenti che consentono di proteggere il computer da virus e malware provenienti da Internet, nonché da accessi di rete indesiderati.
  - Nella rubrica **FireWall** è possibile configurare le impostazioni di base di FireWall. Vengono inoltre visualizzate le attuali velocità di trasferimento dati e tutte le applicazioni attive che utilizzano un collegamento alla rete (vedere FireWall).
  - La rubrica Web Protection visualizza informazioni sugli URL scansionati e sui virus individuati, nonché ulteriori dati statistici, che possono essere ripristinati in qualsiasi momento e consente di richiamare il file di report. Informazioni dettagliate sull'ultimo virus o programma indesiderato trovato sono reperibili premendo un pulsante.
  - La rubrica **Mail Protection** mostra le e-mail verificate, le loro proprietà e altri dati statistici. Inoltre, è possibile spostareescludere per il futuro indirizzi e-mail dalla scansione per malware o spam. Le e-mail possono essere eliminate anche dalla memoria temporanea di Mail Protection. Vedere Mail Protection.
- *PROTEZIONE DEI BAMBINI*: contiene i tool per consentire ai bambini di navigare su Internet in sicurezza.
  - Safe Browsing: è possibile assegnare ruoli utente agli utenti del computer. Il ruolo utente può essere configurato e comprende un set di regole con i seguenti criteri: URL vietati e consentiti (indirizzi Internet), categorie di contenuti vietate, durata di permanenza su Internet ed eventualmente periodi di utilizzo consentiti per i giorni della settimana
- *PROTEZIONE MOBILE*: dalla categoria Avira Free Android Security è possibile accedere online ai dispositivi Android.
  - Avira Free Android Security consente di amministrare tutti i dispositivi basati sul sistema operativo Android.
- *AMMINISTRAZIONE*: contiene i tool per l'isolamento e l'amministrazione dei file sospetti o infetti e la pianificazione delle attività ricorrenti.
  - Nella rubrica **Quarantena** è disponibile il cosiddetto Gestore della quarantena, la postazione centrale per i file già in quarantena o per file sospetti che si desidera spostare in quarantena (vedere Quarantena). Inoltre esiste la possibilità di inviare un file selezionato per e-mail all'Avira Malware Research Center.
  - La rubrica **Pianificatore** consente di creare job temporizzati di controllo e di aggiornamento nonché di backup e di cancellare o modificare job esistenti (vedere Pianificatore).
  - La rubrica **Report** consente di visualizzare i risultati delle azioni eseguite (vedere Report).
  - La rubrica **Eventi** consente di ottenere informazioni sugli eventi generati dai moduli del programma (vedere Eventi).

4.1.2 Configurazione

In Configurazione è possibile effettuare le impostazioni per il prodotto Avira in uso. Dopo l'installazione, il prodotto Avira è configurato con le impostazioni standard che assicurano la protezione ottimale del computer. Ciononostante, il computer o le richieste dell'utente per il prodotto Avira possono possedere caratteristiche particolari e richiedere un adattamento delle componenti di protezione del programma.

La Configurazione è strutturata come una finestra di dialogo: con i pulsanti **OK** o **Applica** si memorizzano le impostazioni scelte durante la configurazione, con **Annulla** si rifiutano le impostazioni, con il pulsante **Valori standard** è possibile ripristinare le impostazioni dei valori standard della configurazione. Nella barra di navigazione a sinistra è possibile selezionare singole rubriche di configurazione.

Richiamo della Configurazione

Esistono diverse possibilità per richiamare la configurazione:

- Dal Pannello di controllo di Windows.
- Dal Centro sicurezza PC di Windows a partire da Windows XP Service Pack 2.
- Mediante l'icona della barra delle applicazioni del programma Avira.
- Nel Control Center mediante la voce di menu Extra > Configurazione.

- Nel Control Center mediante il pulsante Configurazione.

> **Nota**
> Se si richiama la configurazione con il pulsante **Configurazione** in Control Center, si giunge nel registro di configurazione della rubrica attiva in Control Center.

Utilizzo della Configurazione

All'interno della finestra di configurazione si può navigare come in Esplora risorse di Windows:

- Fare clic su una voce della struttura ad albero per visualizzare questa categoria di configurazione nella finestra dei dettagli.
- Fare clic sul segno + prima delle voci per estendere la categoria di configurazione e visualizzare le rubriche di configurazione subordinate nella struttura ad albero.
- Per nascondere le rubriche di configurazione subordinate fare clic sul segno - prima della categoria di configurazione estesa.

> **Nota**
> Per attivare o disattivare le opzioni nella Configurazione e per premere i pulsanti, è possibile utilizzare le combinazioni di tasti [**Alt**] + carattere sottolineato nel nome dell'opzione o nella definizione del pulsante.

Se si desidera applicare le impostazioni nella configurazione:

- Fare clic sul pulsante **OK**.

  ↳ La finestra di configurazione viene chiusa e le impostazioni applicate.

  \- OPPURE -

  Fare clic sul pulsante **Applica**.

  ↳ Le impostazioni vengono applicate. La finestra di configurazione rimane aperta.

Se si desidera terminare la configurazione senza applicare le impostazioni:

- Fare clic sul pulsante **Annulla**.

  ↳ La finestra di configurazione si chiude e le impostazioni vengono ignorate.

Se si desidera ripristinare tutte le impostazioni dei valori standard nella configurazione:

- Fare clic su **Valori standard**.

  ↳ Tutte le impostazioni dei valori standard nella configurazione vengono ripristinate. Quando si ripristinano i valori standard tutte le modifiche e le immissioni dell'utente vengono perse.

Opzioni di configurazione in sintesi

Sono disponibili le seguenti opzioni di configurazione:

- **System Scanner**: configurazione della scansione diretta
  - Opzioni di ricerca
  - Azione in caso di rilevamento
  - Opzioni per la scansione degli archivi
  - Eccezioni della scansione diretta
  - Euristica della scansione diretta
  - Impostazione della funzione di report
- **Real-Time Protection**: configurazione della scansione in tempo reale
  - Opzioni di ricerca
  - Azione in caso di rilevamento
  - Altre azioni
  - Eccezioni della scansione in tempo reale
  - Euristica della scansione in tempo reale
  - Impostazione della funzione di report
- **Aggiornamento**: configurazione delle impostazioni di aggiornamento
  - Download tramite server Web
- **Web Protection**: configurazione di Web Protection
  - Opzioni di scansione, attivazione e disattivazione di Web Protection
  - Azione in caso di rilevamento
  - Accessi bloccati: tipi di file e tipi di MIME indesiderati, Filtro Web per URL noti indesiderati (malware, phishing, ecc.)
  - Eccezioni di scansioni di Web Protection: URL, tipi di file, tipi di MIME
  - Euristica di Web Protection
  - Impostazione della funzione di report
- **Mail Protection**: configurazione di Mail Protection
  - Opzioni di scansione: attivazione del monitoraggio degli account POP3, account IMAP e delle e-mail in uscita (SMTP)
  - Azione in caso di rilevamento
  - Altre azioni
  - Euristica della scansione di Mail Protection
  - Funzione AntiBot: server SMTP consentiti, mittenti e-mail consentiti
  - Eccezioni della scansione di Mail Protection
  - Configurazione della memoria temporanea, svuota la memoria temporanea
  - Configurazione di un piè di pagina nelle e-mail inviate
  - Impostazione della funzione di report
- **Protezione dei bambini**:

- Safe Browsing: funzione di protezione dei bambini con filtro basato sui ruoli e limitazione temporale dell'utilizzo di Internet basata sui ruoli

- **Generale**:
  - Categorie estese delle minacce per la scansione diretta e in tempo reale
  - Protezione avanzata: attivazione di ProActiv e Protection Cloud
  - Filtro applicazioni: blocco o autorizzazione delle applicazioni
  - Protezione con password per l'accesso al Control Center e alla configurazione
  - Sicurezza: blocco delle funzioni di esecuzione automatica, blocco dei file host di Windows, protezione del prodotto
  - WMI: attiva supporto WMI
  - Configurazione del log eventi
  - Configurazione delle funzioni di report
  - Impostazione delle directory utilizzate
  - Configurazione degli avvisi acustici in caso di rilevamento malware

4.1.3 Icona della barra delle applicazioni

Dopo l'installazione, l'icona della barra delle applicazioni del prodotto Avira è collocata nella barra delle applicazioni:

Icona	Descrizione
	Avira Real-Time Protection è attivo
	Avira Real-Time Protection non è attivo

L'icona della barra delle applicazioni mostra lo stato di Real-Time Protection .

Le funzioni principali del prodotto Avira sono facilmente accessibili mediante il menu contestuale dell'icona della barra delle applicazioni.

- Per richiamare il menu contestuale, fare clic con il tasto destro del mouse sull'icona della barra delle applicazioni.

Voci del menu contestuale

- **Attiva Real-Time Protection**: attiva o disattiva Avira Real-Time Protection.
- **Attiva Mail Protection**: attiva o disattiva Avira Mail Protection.
- **Attiva Web Protection**: attiva o disattiva Avira Web Protection.
  - **Attiva Windows Firewall**: attiva o disattiva Windows Firewall (questa funzione sarà disponibile a partire da Windows 8).

- **Avvia Avira Ultimate Protection Suite**: apre Control Center.
- **Configura Avira Ultimate Protection Suite : apre la configurazione.**
- **I miei messaggi: apre una finestra con i messaggi più recenti relativi al prodotto Avira.**
- **Le mie impostazioni di comunicazione: apre il Centro Abo per le comunicazioni del prodotto**
- **Avvia l'aggiornamento: avvia un aggiornamento.**
- **Guida in linea: apre la guida in linea.**
- **Informazioni su Avira Ultimate Protection Suite: apre una finestra di dialogo con informazioni sul prodotto Avira: prodotto, versione e licenza.**
- **Avira su Internet: apre il portale Web di Avira su Internet. Il prerequisito essenziale è l'accesso attivo a Internet.**

4.2 Avira SearchFree Toolbar

Avira SearchFree Toolbar contiene due componenti principali: Avira SearchFree e la Toolbar già nota.

La nuova Avira SearchFree Toolbar viene installata come componente aggiuntivo. Quando si richiama per la prima volta il browser (con Internet Explorer e Firefox) verrà chiesto se si consente la modifica del browser dell'utente da parte del programma Avira SearchFree Toolbar. Per terminare con successo l'installazione di Avira SearchFree Toolbar, l'utente dovrà accettare.

Avira SearchFree è il nuovo motore di ricerca di Avira e contiene un logo Avira, su cui si può fare clic, che conduce alla pagina web di Avira e anche in canali web e di immagini. Consente agli utenti di Avira di effettuare una ricerca ampia e sicura.

La Toolbar è integrata nel browser Web ed è formata da un campo di ricerca, un logo Avira collegato alla pagina web di Avira, due display di stato, tre widget e il menu **Opzioni**.

- Barra di ricerca
  Utilizzare la barra di ricerca per effettuare ricerche in Internet in modo veloce e gratuito tramite il motore di ricerca Avira SearchFree.
- Display di stato
  I display di stato indicano lo stato di Web Protection e l'attuale stato di aggiornamento del prodotto Avira, aiutando l'utente a riconoscere quali azioni devono essere eseguite per proteggere il PC.
- Widget
  Avira fornisce un accesso diretto alle funzioni più importanti su Internet, ad esempio alle notizie dell'utente su Facebook o alla sua casella e-mail. È anche possibile determinare la sicurezza del sistema dell'utente attraverso il widget sicurezza del browser (solo per Firefox e Internet Explorer).

- Opzioni
  Tramite il menu Opzioni è possibile accedere alle Opzioni della toolbar, cancellare la cronologia delle ricerche, richiamare la Guida in linea e le Informazioni relative alla toolbar e disinstallare l'Avira SearchFree Toolbar direttamente tramite browser Web (solo per Firefox e Internet Explorer).

4.2.1 Utilizzo

Barra di ricerca

Tramite la barra di ricerca è possibile ricercare su Internet uno o più termini.

Per fare questo inserire il termine desiderato nel campo di ricerca e premere poi il pulsante **Invio** o fare clic su **Cerca**. Il motore di ricerca Avira SearchFree esegue la ricerca su Internet e mostra poi tutti i risultati riscontrati nella finestra del browser.

La procedura per eseguire la configurazione personalizzata di Avira SearchFree in Internet Explorer, Firefox e Chrome è contenuta in **Opzioni.**

Display di stato

Web Protection

Per determinare lo stato di sicurezza del computer, è possibile utilizzare le icone e i messaggi riportati di seguito:

Icona	Display di stato	Descrizione
✔	*Web Protection*	Passando con il puntatore del mouse sul simbolo, appare il seguente avviso: *Avira Web Protection è attiva. Il PC è protetto.* Ciò significa che non sono necessarie ulteriori azioni.
!	*Web Protection*	Passando con il puntatore del mouse sul simbolo, appare il seguente avviso: *Avira Web Protection non è attiva. Per scoprire come attivarla, fai clic qui.* → L'utente verrà indirizzato a un articolo della nostra Knowledge Base.

	Web Protection assente	Passando con il puntatore del mouse sul simbolo, appare il seguente avviso: • *Non hai Avira Web Protection installata. Per scoprire come proteggere la tua navigazione, fai clic qui.* Ciò potrebbe significare che l'antivirus Avira in uso è disinstallato oppure che non è stato installato correttamente. • *Web protection è inclusa gratuitamente nell'antivirus Avira. Per scoprire come installarla, fai clic qui.* Ciò significa che Web Protection non è stata installata oppure che è stata disinstallata. ↳ In entrambi i casi si viene rimandati al sito Web di Avira, da cui è possibile scaricare il prodotto Avira.
	Errore	Passando con il puntatore del mouse sul simbolo, appare il seguente avviso: *Si è verificato un errore in Avira.* ▶ Fai clic qui per contattare l'assistenza e ricevere aiuto.

Widget

Avira SearchFree Toolbar dispone di 3 widget con le più importanti funzioni di Internet: Facebook, e-mail e Web Protection.

Facebook

Questa funzione consente di ricevere direttamente le comunicazioni di Facebook e quindi di rimanere sempre aggiornato.

E-mail

Quando si fa clic sul simbolo e-mail viene visualizzato un elenco a discesa in cui è possibile scegliere tra i provider più utilizzati.

Web Protection

Questo widget è stato sviluppato da Avira per raggiungere in modo particolarmente semplice tutte le opzioni di sicurezza di Internet. Al momento è disponibile soltanto per Firefox e Internet Explorer. Sono offerte differenti opzioni che si possono chiamare in modo differente a seconda del browser:

- *Blocco pop-up*

Se questa opzione è attiva quando si naviga su Internet verranno bloccate tutte le finestre pop-up.

- *Blocco cookie*

Se questa opzione è attiva non verrà salvato alcun cookie durante l'utilizzo del browser.

- *Navigazione anonima (Firefox) / In Private Browsen (Internet Explorer)*

Se questa opzione è attiva, quando si naviga su Internet non si lasciano tracce. Quest'opzione non è disponibile per Internet Explorer 7 e 8.

- *Cancella cronologia recente (Firefox) / Cancellazione della cronologia di navigazione (Internet Explorer)*

Con questa opzione si cancellano tutte le precedenti attività di Internet.

Website Safety Advisor

Website Safety Advisor offre una classificazione della sicurezza durante la navigazione su Internet.
In questo modo è possibile valutare se la pagina Web che si sta visitando rappresenta un rischio basso o elevato per la sicurezza.
Questo widget offre inoltre altre informazioni sul sito Web, ad esempio il proprietario del dominio o il motivo per cui il sito Web è stato inserito in una determinata categoria.
I livelli di sicurezza sono tre: sicuro, poco rischioso e molto rischioso.

I livelli di sicurezza vengono indicati nella toolbar e nei risultati della ricerca, sotto forma dell'icona Avira Tray, con i seguenti simboli:

Icona	Display di stato	Descrizione
	Sicuro	I siti Web sicuri sono contrassegnati da un segno di spunta verde.
	È Rischio Basso	I siti Web moderatamente rischiosi sono contrassegnati da un punto esclamativo giallo.
	È Rischio Elevato	I siti Web molto rischiosi sono contrassegnati dal segnale rosso di stop.
	Mancato	Un punto di domanda grigio indica i siti Web il cui rischio non può essere valutato.

	Verifica	Questo segno compare durante la verifica dello stato.

Browser Tracking Blocker

Con Browser Tracking Blocker è possibile interrompere i rilevamenti delle informazioni relative alla navigazione dell'utente su Internet.
Il widget consente di selezionare quali rilevamenti bloccare e quali consentire.

Le aziende si dividono in tre categorie:

- Social Networks
- Network
- Altre aziende

4.2.2 Opzioni

Avira SearchFree Toolbar è compatibile con Internet Explorer, Firefox e Google Chrome e può essere configurata in entrambi i browser Web in base alle esigenze dell'utente:

- Opzioni di configurazione con Internet Explorer
- Opzioni di configurazione con Firefox
- Opzioni di configurazione con Chrome

Internet Explorer

Nel browser Web Internet Explorer, nel menu **Opzioni**, sono disponibili le seguenti opzioni di configurazione per l'Avira SearchFree Toolbar:

Opzioni della Toolbar

Cerca

Seleziona motore Avira

Nel menu **Seleziona motore Avira** è possibile selezionare quale motore di ricerca deve essere utilizzato per la ricerca. Sono disponibili motori di ricerca delle seguenti zone: USA, Brasile, Germania, Spagna, Europa, Francia, Italia, Paesi Bassi, Russia e Gran Bretagna.

Avvia ricerche in

Nel menu dell'opzione **Avvia ricerche in** è possibile selezionare dove deve essere visualizzato il risultato di una ricerca, se nella **Finestra attiva**, in una **nuova finestra** oppure su una**nuova scheda**.

Mostra ultime ricerche

Se l'opzione **Mostra ultime ricerche** è attiva, sotto al campo di inserimento testo della barra di ricerca vengono visualizzati i termini di ricerca digitati fino a quel momento.

Azzera la cronologia delle ricerche all'uscita del browser

Attivare l'opzione **Azzera la cronologia delle ricerche all'uscita del browser** quando non si vuole salvare la cronologia delle ricerche già effettuate e si desidera che venga cancellata alla chiusura del browser Web.

Altre opzioni

Seleziona lingua Toolbar

In **Seleziona lingua Toolbar** è possibile selezionare la lingua di Avira SearchFree Toolbar. Sono disponibili le versioni in inglese, tedesco, spagnolo, francese, italiano, portoghese e olandese.

> **Nota**
> La lingua preimpostata dell'Avira SearchFree Toolbar corrisponde a quella del programma dell'utente, se disponibile. Se la toolbar non è disponibile nella lingua dell'utente, viene preimpostata la lingua inglese.

Visualizza i nomi dei pulsanti

Disattivare l'opzione **Visualizza i nomi dei pulsanti** se si desidera nascondere il testo accanto alle icone di Avira SearchFree Toolbar.

Azzera cronologia delle ricerche

Attivare l'opzione **Azzera cronologia delle ricerche** se non si desidera salvare le ricerche già eseguite, bensì cancellarle subito.

Aiuto

Fare clic su **Aiuto** per richiamare la pagina Web con le domande frequenti (FAQ) riguardo la toolbar.

Disinstalla

È possibile disinstallare l'Avira SearchFree Toolbar anche direttamente in Internet Explorer: Disinstallazione mediante il browser Web.

Info

Fare clic su **Info** per sapere quale versione di Avira SearchFree Toolbar è installata.

Firefox

Nel browser Web Firefox, nel menu **Opzioni**, sono disponibili le seguenti opzioni di configurazione per l'Avira SearchFree Toolbar:

Opzioni della Toolbar

Cerca

Seleziona motore Avira

Nel menu **Seleziona motore Avira** è possibile selezionare quale motore di ricerca deve essere utilizzato per la ricerca. Sono disponibili motori di ricerca delle seguenti zone: USA, Brasile, Germania, Spagna, Europa, Francia, Italia, Paesi Bassi, Russia e Gran Bretagna.

Mostra ultime ricerche

Se l'opzione **Mostra ultime ricerche** è attiva, è possibile visualizzare i termini di ricerca digitati fino a quel momento, facendo clic sulla freccia nella barra di ricerca. Selezionare uno dei termini se si vuole visualizzare nuovamente il risultato di tale ricerca.

Azzera automaticamente ricerche all'uscita del browser

Attivare l'opzione **Azzera automaticamente ricerche all'uscita del browser** quando non si vuole salvare la cronologia delle ricerche già effettuate e si desidera che venga cancellata alla chiusura del browser Web.

Visualizza i risultati della ricerca Ask quando si digitano parole chiave o URL non validi nella barra degli indirizzi del browser

Se questa opzione è attiva, ogni volta che parole chiave o indirizzi URL non validi vengono inseriti nel campo degli indirizzi del browser, viene avviata una ricerca e mostrati i relativi risultati.

Altre opzioni

Seleziona lingua Toolbar

In **Seleziona lingua Toolbar** è possibile selezionare la lingua di Avira SearchFree Toolbar. Sono disponibili le versioni in inglese, tedesco, spagnolo, francese, italiano, portoghese e olandese.

> **Nota**
> La lingua preimpostata dell'Avira SearchFree Toolbar corrisponde a quella del programma dell'utente, se disponibile. Se la toolbar non è disponibile nella lingua dell'utente, viene preimpostata la lingua inglese.

Visualizza i nomi dei pulsanti

Disattivare l'opzione **Visualizza i nomi dei pulsanti** se si desidera nascondere il testo accanto alle icone di Avira SearchFree Toolbar.

Azzera cronologia delle ricerche

Attivare l'opzione **Azzera cronologia delle ricerche** se non si desidera salvare le ricerche già eseguite, bensì cancellarle subito.

Aiuto

Fare clic su **Aiuto** per richiamare la pagina Web con le domande frequenti (FAQ) riguardo la toolbar.

Disinstalla

È possibile disinstallare l'Avira SearchFree Toolbar anche direttamente in Internet Explorer: Disinstallazione mediante il browser Web.

Info

Fare clic su **Info** per sapere quale versione di Avira SearchFree Toolbar è installata.

Chrome

Nel browser Web Google Chrome tutte le opzioni di configurazione sono sotto l'ombrello rosso di Avira. Per l'Avira SearchFree Toolbar sono disponibili le seguenti opzioni:

Aiuto

Fare clic su **Aiuto** per richiamare la pagina Web con le domande frequenti (FAQ) riguardo la toolbar.

Istruzioni per la disinstallazione

Qui è possibile trovare i collegamenti alle istruzioni sulla disinstallazione di Avira SearchFree Toolbar.

Info

Fare clic su **Info** per sapere quale versione di Avira SearchFree Toolbar è installata.

Mostra e nascondi Avira SearchFree Toolbar

Questa voce del menu attiva e disattiva Avira SearchFree Toolbar, che si trova nella parte alta della finestra.

4.2.3 Disinstallazione di Avira SearchFree Toolbar in Windows 7

Per disinstallare Avira SearchFree Toolbar:

- Chiudere il browser Web.

Aprire nel menu **Start** di Windows il **Pannello di controllo**.

Fare doppio clic su **Programmi e funzionalità**.

Selezionare Avira SearchFree Toolbar plus Web Protection nell'elenco e fare clic su **Disinstalla**.

Verrà chiesto all'utente se desidera davvero disinstallare il prodotto.

Confermare con **Sì**.

Avira SearchFree Toolbar plus Web Protection viene disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro di Avira SearchFree Toolbar plus Web Protection vengono eliminate.

4.3 Come procedere

Nei capitoli "Come procedere" viene fornita una breve panoramica dell'attivazione della licenza e del prodotto e delle funzioni principali del prodotto Avira in uso. I brevi passaggi selezionati permettono di farsi un'idea delle funzionalità del prodotto Avira. Tali passaggi non sostituiscono tuttavia le spiegazioni complete nei singoli capitoli della guida.

4.3.1 Attiva licenza

Per attivare la licenza del prodotto Avira in uso, effettuare le seguenti operazioni:

Attivare la licenza per il prodotto Avira con il file di licenza *.KEY*. È possibile ottenere il file di licenza tramite email da Avira. Il file di licenza contiene la licenza per tutti i prodotti che si acquistano con un unico ordine.

Se il prodotto Avira in uso non è ancora stato installato:

- Salvare il file di licenza in una directory locale sul computer.
- Installare il prodotto Avira.
- Durante l'installazione indicare dove è stato memorizzato il file di licenza.

Se il prodotto Avira è stato già installato:

- Fare doppio clic sul file di licenza nel filemanager o nell'email di attivazione e seguire le istruzioni visualizzate dal sistema di gestione delle licenze.

  - OPPURE -

  Nel Control Center del prodotto Avira, selezionare la voce di menu **Guida > Gestione delle licenze**

> **Nota**
> In Windows Vista e versioni successive viene visualizzata la finestra di dialogo Controllo dell'account utente. Registrarsi come amministratore. Fare clic su **Continua**.

- Selezionare il file di licenza e fare clic su **Apri**.
  - ↳ Apparirà un messaggio.
- Confermare con **OK**.
  - ↳ La licenza è attivata.
- Se necessario, riavviare il sistema.

4.3.2 Attivazione del prodotto

Per attivare il prodotto Avira in uso sono disponibili le seguenti opzioni:

- Attivazione con una licenza completa valida

  Per attivare il programma con una licenza completa, è necessario disporre di un codice di attivazione valido che comprende i dati della licenza acquistata. Il codice di attivazione è stato inviato per e-mail oppure è indicato sulla confezione del prodotto.

- Attivazione con una licenza di evaluation

  Il prodotto Avira viene attivato tramite una licenza di evaluation generata automaticamente che consente all'utente di testare il prodotto Avira e tutte le relative funzioni per un periodo di tempo limitato.

> **Nota**
> Per attivare il prodotto o richiedere una licenza di prova, è necessario disporre di una connessione Internet attiva.
> Qualora fosse impossibile connettersi ai server Avira, controllare le impostazioni del firewall utilizzato: per l'attivazione del prodotto vengono utilizzati i collegamenti tramite il protocollo HTTP e la porta 80 (comunicazione Web) e tramite il protocollo di crittografia SSL e la porta 443. Assicurarsi che il proprio firewall non blocchi i dati in entrata o in uscita. Controllare inoltre che il proprio browser Web sia in grado di richiamare pagine Web.

Come attivare il prodotto Avira:

Se il prodotto Avira non è ancora stato installato:

- Installare il prodotto Avira.
  - ↳ Durante l'installazione viene richiesto all'utente di selezionare un'opzione di attivazione
- **Attiva prodotto** = attivazione con una licenza completa valida
- **Prova il prodotto** = attivazione con una licenza di evaluation
- Per l'attivazione con una licenza completa, inserire il codice di attivazione.
- Confermare la scelta della procedura di attivazione con **Avanti**.
- Inserire eventualmente i propri dati personali per la registrazione e confermare con **Avanti**.

↳ Nella finestra di dialogo seguente vengono visualizzati i dati di licenza dell'utente. Il prodotto Avira è stato attivato.

- Continuare l'installazione.

Se il prodotto Avira è già stato installato:

- In Control Center selezionare la voce di menu **Guida in linea > Gestione delle licenze**.

  ↳ Verrà avviato l'assistente per l'installazione della licenza, con cui è possibile selezionare un'opzione di attivazione. I passaggi successivi per l'attivazione del prodotto sono analoghi alla procedura descritta in precedenza.

4.3.3 Esecuzione degli aggiornamenti automatici

Per creare con Avira Pianificatore un job con cui aggiornare automaticamente il prodotto Avira in uso:

- Selezionare la rubrica *AMMINISTRAZIONE* **> Pianificatore** in Control Center.
- Fare clic sull'icona + **Inserisci un nuovo job**.

  ↳ Verrà visualizzata la finestra di dialogo **Nome e descrizione del job**.
- Assegnare un nome al job ed eventualmente descriverlo.
- Fare clic su **Avanti**.

  ↳ Verrà visualizzata la finestra di dialogo **Tipo di job**.
- Selezionare un **Job di aggiornamento** dalla lista.
- Fare clic su **Avanti**.

  ↳ Verrà visualizzata la finestra di dialogo **Durata del job**.
- Selezionare quando deve essere eseguito l'aggiornamento:

- **Immediatamente**
- **Ogni giorno**
- **Ogni settimana**
- **Intervallo**
- **Singolo**
- **Login**

> **Nota**
> Si consiglia di eseguire regolarmente e spesso aggiornamenti automatici. L'intervallo di aggiornamento consigliato è: 2 ore.

- Indicare il termine in base alla selezione.

- Eventualmente selezionare anche le seguenti opzioni aggiuntive (disponibili in base al tipo di job):

- **Ripeti il job a tempo già scaduto**
  Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.
- **Avvia job se è presente una connessione Internet (dial-up)**
  Oltre alla frequenza stabilita il job viene eseguito quando si attiva una connessione a Internet.

- Fare clic su **Avanti**.

  ↳ Verrà visualizzata la finestra di dialogo **Selezione della modalità di visualizzazione**.

- Selezionare la modalità di visualizzazione della finestra del job:

- **Invisibile**: nessuna finestra del job
- **Ridotto**: solo la barra di avanzamento
- **Espanso**: tutta la finestra del job

- Fare clic su **Fine**.

  ↳ Il nuovo job creato viene visualizzato nella schermata iniziale della rubrica *AMMINISTRAZIONE* > **Pianificatore** come attivato (segno di spunta).

- Disattivare i job che non devono essere eseguiti.

Mediante le seguenti icone, è possibile elaborare ulteriormente i job:

Visualizzazione delle proprietà di un job

Modifica del job

Eliminazione del job

Avvio del job

Interruzione del job

4.3.4 Avvio di un aggiornamento manuale

Esistono vari modi di avviare manualmente un aggiornamento: durante gli aggiornamenti avviati manualmente viene sempre eseguito anche l'aggiornamento del file di definizione dei virus e del motore di ricerca.

Per avviare manualmente un aggiornamento del prodotto Avira:

- Fare clic con il tasto destro del mouse sull'icona Tray di Avira nella barra delle applicazioni e selezionare **Avvia aggiornamento**.

  - OPPURE -

- In Control Center selezionare la rubrica **Stato**, quindi fare clic sul link **Avvia aggiornamento** nel riquadro **Ultimo aggiornamento**.

  - OPPURE -

  In Control Center, nel menu **Aggiornamento**, selezionare il comando **Avvia aggiornamento**.

  ↪ Verrà visualizzata la finestra di dialogo **Updater**.

> **Nota**
> Si consiglia di eseguire regolarmente aggiornamenti automatici. L'intervallo di aggiornamento consigliato è: 2 ore.

> **Nota**
> È possibile eseguire un aggiornamento anche manualmente mediante il Centro di sicurezza PC di Windows.

4.3.5 Scansione diretta: scansione di virus e malware con un profilo di scansione

Un profilo di scansione è un insieme di drive e directory che devono essere scansionati.

Per effettuare una scansione con un profilo di scansione è possibile:

Utilizzare il profilo di scansione predefinito

Se i profili di scansione predefiniti rispondono alle esigenze dell'utente.

Modificare il profilo di scansione e utilizzarlo (selezione manuale)

Se si desidera eseguire una scansione con un profilo di scansione personalizzato.

Creare e utilizzare un nuovo profilo di scansione

Se si desidera creare un profilo di scansione personale.

In base al sistema operativo sono disponibili diverse icone per l'avvio di un profilo di scansione:

- In Windows XP:

  Con quest'icona si avvia la scansione mediante un profilo di scansione.

- In Windows Vista e versioni successive:

In Microsoft Windows Vista e versioni successive, il Control Center ha inizialmente solo diritti limitati, ad esempio per l'accesso a file e directory. Alcune azioni e l'accesso ai file possono essere eseguiti dal Control Center solo con diritti di amministratore avanzati. Questi diritti di amministratore avanzati devono essere assegnati a ogni avvio di una scansione mediante un profilo di scansione.

- Selezionando quest'icona si avvia una scansione limitata mediante un profilo di scansione. Vengono scansionati solo i file e le directory per i quali il sistema operativo ha concesso i diritti di accesso.
- Con quest'icona si avvia una scansione con diritti avanzati dell'amministratore. Dopo una conferma, vengono scansionati tutti i file e le directory del profilo di scansione selezionato.

Per cercare virus e malware con un profilo di scansione:

- In Control Center selezionare la rubrica *SICUREZZA DEL COMPUTER* **> System Scanner**.

  ↳ Verranno visualizzati i profili di scansione predefiniti.

- Selezionare uno dei profili di scansione predefiniti.

  - OPPURE -

  Modificare il profilo di scansione in **Selezione manuale**.

  - OPPURE -

  Creare un nuovo profilo di scansione

- Fare clic sull'icona (Windows XP: o Windows Vista e versioni successive:).
- Verrà visualizzata la finestra **Luke Filewalker** e si avvierà la scansione diretta.

  ↳ Al termine del processo di scansione vengono visualizzati i risultati.

Se si desidera modificare un profilo di scansione:

- Aprire nel profilo di scansione **Selezione manuale** la struttura dei file fino a che non vengono aperti tutti i drive e le directory che devono essere scansionati.

- Fare clic sul segno **+**: viene visualizzato il livello successivo della directory.
- Fare clic sul segno **-**: viene nascosto il livello successivo della directory.

- Evidenziare i nodi e le directory da scansionare facendo clic sulla casella corrispondente del livello della directory appropriato:

  Sono disponibili le seguenti possibilità per selezionare le directory:

- Directory incluse le sottodirectory (segno di spunta nero)
- Solo le sottodirectory in una directory (segno di spunta grigio, le sottodirectory hanno un segno di spunta nero)
- Nessuna directory (nessun segno di spunta)

Se si desidera creare un nuovo profilo di scansione:

- Fare clic sull'icona **Crea nuovo profilo.**
  - ↳ Il profilo **Nuovo profilo** viene visualizzato sotto i profili già esistenti.
- Assegnare un nome al profilo di scansione con un clic sul simbolo .
- Evidenziare altri nodi e directory da salvare con un clic nella checkbox del livello della directory corrispondente.

  Sono disponibili le seguenti possibilità per selezionare le directory:

- Directory incluse le sottodirectory (segno di spunta nero)
- Solo le sottodirectory in una directory (segno di spunta grigio, le sottodirectory hanno un segno di spunta nero)
- Nessuna directory (nessun segno di spunta)

4.3.6 Scansione diretta: ricerca di virus e malware con Drag&Drop

È possibile cercare con Drag&Drop virus e malware come segue:

✓ Il Control Center del programma Avira è aperto.

- Selezionare il file o la directory, che si desidera scansionare.
- Trascinare con il tasto sinistro del mouse il file selezionato o la directory in Control Center.
  - ↳ Verrà visualizzata la finestra **Luke Filewalker** e si avvierà la scansione diretta.
  - ↳ Al termine del processo di scansione vengono visualizzati i risultati.

4.3.7 Scansione diretta: Scansione di virus e malware con il menu contestuale

Per eseguire una scansione mirata in cerca di virus e malware mediante il menu contestuale:

- Fare clic (ad esempio in Esplora risorse di Windows, sul desktop o in una directory aperta di Windows) con il pulsante destro del mouse sul file o sulla directory che si desidera controllare.
  - ↳ Verrà visualizzato il menu contestuale di Esplora risorse di Windows.
- Nel menu contestuale selezionare **Controlla i file selezionati con Avira**.
  - ↳ Verrà visualizzata la finestra **Luke Filewalker** e si avvierà la scansione diretta.
  - ↳ Al termine del processo di scansione vengono visualizzati i risultati.

4.3.8 Scansione diretta: ricerca automatica di virus e malware

> **Nota**
> Dopo l'installazione, il job di scansione *Scansione completa del sistema* viene creato nel pianificatore: la scansione completa del sistema viene eseguita automaticamente alla frequenza consigliata.

Come creare un job di scansione automatica di virus e malware:

- Selezionare la rubrica *AMMINISTRAZIONE* **> Pianificatore** in Control Center.
- Fare clic sull'icona [+] **Inserisci un nuovo job**.
  - ↳ Verrà visualizzata la finestra di dialogo **Nome e descrizione del job**.
- Assegnare un nome al job ed eventualmente descriverlo.
- Fare clic su **Avanti**.
  - ↳ Verrà visualizzata la finestra di dialogo **Tipo di job**.
- Selezionare il **Job di scansione**.
- Fare clic su **Avanti**.
  - ↳ Verrà visualizzata la finestra di dialogo **Selezione del profilo**.
- Selezionare quale profilo deve essere scansionato.
- Fare clic su **Avanti**.
  - ↳ Verrà visualizzata la finestra di dialogo **Durata del job**.
- Selezionare quando deve essere eseguita la scansione:

- **Immediatamente**
- **Ogni giorno**
- **Ogni settimana**
- **Intervallo**
- **Singolo**
- **Login**

- Indicare il termine in base alla selezione.
- Eventualmente selezionare la seguente opzione supplementare (disponibile in base al tipo di job): **Ripeti il job a tempo già scaduto**
  - ↳ Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.
- Fare clic su **Avanti**.
  - ↳ Verrà visualizzata la finestra di dialogo **Selezione della modalità di visualizzazione**.
- Selezionare la modalità di visualizzazione della finestra del job:

- **Invisibile**: nessuna finestra del job
- **Ridotto**: solo la barra di avanzamento
- **Espanso**: tutta la finestra del job

- Selezionare l'opzione **Spegni computer al termine del job** se si desidera che il computer si spenga automaticamente non appena il job è stato eseguito e concluso.

  L'opzione è disponibile solo nella modalità di visualizzazione ridotta o estesa.

- Fare clic su **Fine**.

  ↳ Il nuovo job creato viene visualizzato nella schermata iniziale della rubrica *AMMINISTRAZIONE* **> Pianificatore** come attivato (segno di spunta).

- Disattivare i job che non devono essere eseguiti.

Mediante le seguenti icone, è possibile elaborare ulteriormente i job:

Visualizzazione delle proprietà di un job

Modifica del job

Eliminazione del job

Avvio del job

Interruzione del job

4.3.9 Scansione diretta: scansione mirata in cerca di rootkit attivi

Per effettuare una scansione in cerca di rootkit attivi utilizzare il profilo di scansione predefinito **Scansione alla ricerca di rootkit e malware attivi**.

La ricerca di rootkit mirata si effettua nel modo seguente:

- Selezionare la rubrica *SICUREZZA DEL COMPUTER* **> System Scanner**.

  ↳ Verranno visualizzati i profili di scansione predefiniti.

- Selezionare il profilo di scansione predefinito **Scansione alla ricerca di rootkit e malware attivi**.

- Evidenziare altri eventuali nodi e directory da verificare con un clic nella casella del livello della directory.

- Fare clic sull'icona (Windows XP: o Windows Vista e sistemi operativi successivi:).

  ↳ Verrà visualizzata la finestra **Luke Filewalker** e si avvierà la scansione diretta.

↳ Al termine del processo di scansione vengono visualizzati i risultati.

4.3.10 Reazione a virus e malware riscontrati

Per i singoli componenti di protezione del prodotto Avira è possibile impostare nella configurazione, nella rubrica **Azione in caso di rilevamento**, la reazione desiderata del prodotto Avira in caso di rilevamento di un virus o di un programma indesiderato.

Nel componente ProActiv di Real-Time Protection non esiste la possibilità di configurare alcuna opzione di azione: i rilevamenti vengono sempre comunicati nella finestra **Real-Time Protection: Comportamento sospetto da parte di un'applicazione**.

Opzioni di azione in Scanner:

- **Interattivo**

  Nella modalità di azione interattiva vengono comunicati i rilevamenti della scansione di Scanner in una finestra di dialogo. Questa impostazione è attivata di default.
  Al termine della **scansione di Scanner**, si riceve un avviso con l'elenco dei file infetti rilevati. Mediante il menu contestuale è possibile selezionare un'azione da eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure chiudere Scanner.

- **Automatico**

  Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Opzioni di azione in Real-Time Protection:

- **Interattivo**

  Nella modalità di azione interattiva viene negato l'acceso ai dati e sul desktop viene visualizzato un messaggio. È possibile rimuovere il malware rilevato direttamente nel messaggio sul desktop, oppure trasmetterlo al componente Scanner per un ulteriore trattamento del virus selezionando il pulsante **Dettagli**. Scanner notifica il rilevamento tramite una finestra con un menu contestuale contenente diverse opzioni per trattare il file infetto (vedere Rilevamento > Scanner).

- **Automatico**

  Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato, l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Opzioni di azione in Mail Protection, Web Protection:

- **Interattivo**

  Nella modalità di azione interattiva, in caso di rilevamento di un virus o di un programma indesiderato appare una finestra di dialogo nella quale è possibile scegliere come gestire i file infetti. Questa impostazione è attivata di default.

- **Automatico**

Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Modalità di azione interattiva

- Nella modalità di azione interattiva si reagisce ai virus e ai programmi indesiderati rilevati selezionando nell'avviso un'**azione per gli oggetti infetti** ed eseguendo l'azione selezionata mediante **Conferma**.

Per il trattamento di oggetti infetti possono essere selezionate le seguenti azioni:

> **Nota**
> Le azioni disponibili dipendono dal sistema operativo, dal componente di protezione (Avira Scanner, Avira Real-Time Protection, Avira Mail Protection, Avira Web Protection), che segnala il file rilevato, e dal malware rilevato.

Azioni di Scanner e di Real-Time Protection (senza rilevamenti da parte di ProActiv):

- **Ripara**

  Il file viene riparato.
  Questa opzione è attivabile solo se è possibile riparare il file.

- **Rinomina**

  Il file viene rinominato in **.vir*. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere successivamente riparati e nuovamente rinominati.

- **Quarantena**

  Il file viene compresso in un formato speciale (**.qua*) e spostato nella directory di quarantena *INFECTED* sull'hard disk, in modo da escludere qualsiasi accesso diretto. I file in questa directory possono essere successivamente riparati nella quarantena o, se necessario, inviati ad Avira.

- **Elimina**

  Il file viene eliminato. Questa procedura è molto più rapida di **Sovrascrivi ed elimina**.
  Se il file rilevato è un virus del record di avvio, eliminandolo viene cancellato il record di avvio. Viene scritto un nuovo record di avvio.

- **Ignora**

  Non vengono eseguite ulteriori azioni. Il file infetto rimane attivo sul computer.

- **Sovrascrivi ed elimina**

  Il file viene sovrascritto con un modello e, infine, eliminato. Il file non può essere ripristinato.

> **Avviso**
> Pericolo di perdita di dati e danni al sistema operativo del computer!
> Utilizzare l'opzione **Ignora** solo in casi eccezionali e fondati.

- **Ignora sempre**

  Opzione di azione in caso di rilevamento di Real-Time Protection: Real-Time Protection non esegue nessun'altra azione. L'accesso al file è consentito. Tutti gli ulteriori accessi a questo file sono consentiti e non vengono più segnalati fino al riavvio del computer o all'aggiornamento del file di definizione dei virus.

- **Copia in quarantena**

  Opzione di azione in caso di rilevamento di un rootkit: il rilevamento viene copiato in quarantena.

- **Ripara record di avvio | Scarica strumento di riparazione**

  Opzioni di azione in caso di rilevamento di record di avvio: sono disponibili opzioni per la riparazione per le unità floppy infette. Se con il prodotto Avira non è possibile effettuare alcuna riparazione, è possibile scaricare uno strumento speciale che riconosce e rimuove i virus del record di avvio.

> **Nota**
> Se si applicano azioni su processi in corso, i processi interessati vengono terminati prima dell'esecuzione dell'azione.

Azioni di Real-Time Protection in caso di rilevamento dei componenti ProActiv (notifica di azioni sospette di un'applicazione):

- **Programma attendibile**

  L'esecuzione dell'applicazione prosegue. Il programma viene inserito nell'elenco delle applicazioni consentite ed escluso dal monitoraggio mediante il componente ProActiv. Aggiungendolo nell'elenco delle applicazioni consentite viene impostato il tipo di monitoraggio *Contenuti*. Questo significa che l'applicazione viene esclusa dal monitoraggio mediante il componente ProActiv solo in caso di contenuti non modificati (vedere Filtro applicazioni: Applicazioni consentite).

- **Blocca il programma una volta**

  L'applicazione viene bloccata, quindi l'esecuzione dell'applicazione viene terminata. Le azioni dell'applicazione continuano a essere monitorate dal componente ProActiv.

- **Blocca sempre questo programma**

  L'applicazione viene bloccata, quindi l'esecuzione dell'applicazione viene terminata. Il programma viene inserito nell'elenco delle applicazioni da bloccare e non può più essere eseguito (vedere Filtro applicazione: applicazioni da bloccare).

- **Ignora**

  L'esecuzione dell'applicazione prosegue. Le azioni dell'applicazione continuano a essere monitorate dal componente ProActiv.

Azioni di Mail Protection: e-mail in ingresso

- **Sposta in quarantena**

  L'e-mail viene spostata in Quarantena unitamente a tutti gli allegati. L'e-mail infetta viene eliminata. Il corpo del testo delle e-mail e gli eventuali allegati vengono sostituiti da un testo standard.

- **Elimina e-mail**

  L'e-mail infetta viene eliminata. Il corpo del testo e gli eventuali allegati delle e-mail vengono sostituiti da un testo standard.

- **Elimina allegato**

  L'allegato infetto viene sostituito da un testo standard. Se il corpo del testo dell'e-mail risulta infetto, viene eliminato ed eventualmente sostituito da un testo standard. L'e-mail stessa viene inoltrata.

- **Sposta allegato in quarantena**

  L'allegato infetto viene collocato in Quarantena e infine eliminato (sostituito da un testo standard). Il corpo dell'e-mail viene inoltrato. L'allegato infetto potrà essere successivamente inoltrato con il Gestore della quarantena.

- **Ignora**

  L'e-mail infetta viene inoltrata.

> **Avviso**
> In questo modo virus e programmi indesiderati potrebbero accedere al computer. Selezionare l'opzione **Ignora** solo in casi eccezionali e fondati. Disattivare l'anteprima in Microsoft Outlook, non aprire mai gli allegati facendo doppio clic!

Azioni di Mail Protection: e-mail in uscita

- **Sposta e-mail in quarantena (non inviare)**

  L'e-mail, unitamente agli allegati, viene copiata in Quarantena e non inviata. L'e-mail resta nella Posta in uscita del client e-mail. Nel programma e-mail viene visualizzato un messaggio di errore. In tutte le procedure di invio seguenti dell'account di posta elettronica questo messaggio viene verificato per malware.

- **Blocca invio e-mail (non inviare)**

  L'e-mail non viene inviata e resta nella Posta in uscita del client e-mail. Nel programma e-mail viene visualizzato un messaggio di errore. In tutte le procedure di invio seguenti dell'account di posta elettronica questo messaggio viene verificato per malware.

- **Ignora**

  Le e-mail infette vengono inviate.

> **Avviso**
> In questo modo virus e programmi indesiderati potrebbero raggiungere il computer del destinatario dell'e-mail.

Azioni di Web Protection:

- **Nega accesso**

  Il sito Web richiesto dal server Web o i dati e i file trasferiti non vengono inviati al proprio browser Web. Nel browser Web viene visualizzato un messaggio di errore relativo al divieto di accesso.

- **Quarantena**

  Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono spostati nella quarantena. Il file infetto può essere ripristinato dal Gestore della quarantena se ha un valore informativo, oppure, se necessario, inviato ad Avira Malware Research Center.

- **Ignora**

  Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inoltrati da Web Protection al proprio browser Web.

> **Avviso**
> In questo modo virus e programmi indesiderati potrebbero accedere al computer. Selezionare l'opzione **Ignora** solo in casi eccezionali e fondati.

> **Nota**
> Consigliamo di spostare in quarantena un file sospetto che non può essere riparato.

> **Nota**
> Inviare a noi i file da analizzare che sono stati segnalati dall'euristica.
> Sul nostro sito Web http://www.avira.com/sample-upload
> è possibile caricare ad esempio i file segnalati dall'euristica, riconoscibili dal prefisso *HEUR/* o *HEURISTIC/* anteposto al nome, ad esempio *HEUR/filediprova.**.

4.3.11 Quarantena: trattamento dei file (*.qua) in quarantena

È possibile trattare i file in quarantena nel modo seguente:

- Selezionare la rubrica *AMMINISTRAZIONE* **> Quarantena** in Control Center.

- Verificare di quali file si tratta cosicché sia possibile ripristinare gli originali sul computer.

Se si desidera visualizzare maggiori informazioni su un file:

- Selezionare il file e fare clic su .
  - ↳ Verrà visualizzata la finestra di dialogo **Proprietà** con ulteriori informazioni sul file.

Se si desidera scansionare nuovamente un file:

La scansione di un file è consigliata quando il file di definizione dei virus del prodotto Avira è stato aggiornato ed esiste il sospetto di un falso allarme. È così possibile confermare un falso allarme a una successiva verifica e ripristinare il file.

- Selezionare il file e fare clic su .
  - ↳ Il file viene controllato utilizzando le impostazioni della scansione diretta per virus e malware.
  - ↳ Dopo il controllo appare la finestra di dialogo **Statistiche della scansione** in cui viene visualizzata la statistica relativa allo stato del file prima e dopo la nuova scansione.

Se si desidera eliminare un file:

- Selezionare il file e fare clic su .
- Confermare la selezione con **Sì**.

Se si desidera caricare il file da analizzare su un server Web di Avira Malware Research Center:

- Selezionare il file che si desidera caricare.
- Fare clic su .
  - ↳ Si aprirà la finestra di dialogo *Upload file* con un modulo per inserire i dati personali a cui essere contattati.
- Indicare per intero i propri dati.
- Scegliere un tipo:: **File sospetto** o **Sospetto di falso positivo**.
- Selezionare un formato di risposta: **HTML**, **Testo**, **HTML & Testo**.
- Fare clic su **OK.**
  - ↳ Il file compresso viene caricato su un server Web di Avira Malware Research Center.

> **Nota**
> Nei seguenti casi si consiglia di eseguire un'analisi con Avira Malware Research Center:
> **Riscontro euristico (file sospetto)**: Durante una scansione un file è stato classificato come sospetto dal prodotto Avira in uso e messo in quarantena: nella finestra di dialogo sul rilevamento del virus oppure nel file di report della scansione viene consigliato di analizzare il file con Avira Malware Research Center.
> **File sospetto**: Il file ritenuto sospetto è stato aggiunto alla quarantena, tuttavia la ricerca di virus e malware nel file ha dato esito negativo.
> **Sospetto di falso positivo**: si presume che il virus trovato sia un falso positivo: il prodotto Avira indica un rilevamento in un file che però molto probabilmente non è infetto da malware.

> **Nota**
> La dimensione dei file caricati si limita a 20 MB non compressi o a 8 MB compressi.

> **Nota**
> È possibile caricare solo un singolo file per volta.

Se si desidera copiare un oggetto in quarantena dalla quarantena a un'altra directory:

- Selezionare l'oggetto in quarantena e fare clic su .
  - ↳ Si apre la finestra di dialogo *Cerca cartella* in cui è possibile selezionare una directory.
- Selezionare una directory nella quale deve essere archiviata una copia dell'oggetto in quarantena e confermare con **OK**.
  - ↳ L'oggetto in quarantena selezionato viene archiviato nella directory scelta.

> **Nota**
> L'oggetto in quarantena non corrisponde esattamente al file ripristinato. L'oggetto in quarantena è crittografato e non può essere eseguito o letto nel formato originale.

Se si desidera esportare in un file di testo le proprietà di un oggetto in quarantena selezionato:

- Selezionare l'oggetto in quarantena e fare clic su .

↳ Si apre un file di testo con i dati dell'oggetto in quarantena scelto.

- Salvare il file di testo.

I file in quarantena possono essere ripristinati (vedere capitolo: Quarantena: ripristino dei file in quarantena).

4.3.12 Quarantena: ripristino dei file in quarantena

In base al sistema operativo sono disponibili diverse icone per il ripristino:

- In Windows XP:
  - Quest'icona consente di ripristinare i file nella directory originale.
  - Quest'icona consente di ripristinare i file nella directory selezionata.
- In Windows Vista e versioni successive:

  In Microsoft Windows Vista e versioni successive, il Control Center ha inizialmente solo diritti limitati, ad esempio per l'accesso a file e directory. Alcune azioni e l'accesso ai file possono essere eseguiti dal Control Center solo con diritti di amministratore avanzati. Questi diritti di amministratore avanzati devono essere assegnati a ogni avvio di una scansione mediante un profilo di scansione.
  - Quest'icona consente di ripristinare i file nella directory selezionata.
  - Quest'icona consente di ripristinare i file nella directory originale. Se per l'accesso a questa directory sono necessari diritti di amministratore avanzati, appare una richiesta corrispondente.

È possibile ripristinare i file in quarantena nel modo seguente:

> **Avviso**
> Pericolo di perdita di dati e danni al sistema operativo del computer! Utilizzare la funzione **Ripristina l'oggetto selezionato** solo in casi eccezionali. Ripristinare solo quei file che possono essere riparati con una nuova scansione.

✓ File nuovamente scansionato e riparato con una scansione.

- Selezionare la rubrica *AMMINISTRAZIONE* **> Quarantena** in Control Center.

> **Nota**
> Le email e i relativi allegati possono essere ripristinati soltanto con l'opzione e con l'estensione **.eml*.

Se si desidera ripristinare un file nella sua posizione originale:

- Evidenziare il file e fare clic sull'icona (Windows XP: , Windows Vista e versioni successive).

Questa opzione non è disponibile per le email.

> **Nota**
> Le email e i relativi allegati possono essere ripristinati soltanto con l'opzione e con l'estensione **.eml*.

↳ Viene richiesto quindi se si desidera ripristinare il file.

- Fare clic su **Sì**.

↳ Il file viene ripristinato nella directory dalla quale è stato spostato in quarantena.

Se si desidera ripristinare un file in una determinata directory:

- Selezionare il file e fare clic su .

↳ Viene richiesto quindi se si desidera ripristinare il file.

- Fare clic su **Sì**.

↳ Viene visualizzata la finestra di default di Windows *Salva con nome* per la selezione di una directory.

- Selezionare la directory nella quale si desidera ripristinare il file e confermare.

↳ Il file viene ripristinato nella directory selezionata.

4.3.13 Quarantena: spostamento dei file sospetti in quarantena

È possibile spostare in quarantena i file sospetti manualmente come segue:

- Selezionare la rubrica *AMMINISTRAZIONE* **> Quarantena** in Control Center.
- Fare clic su + .

↳ Apparirà la finestra standard di Windows per la selezione di un file.

- Selezionare il file e confermare facendo clic su **Apri**.

↳ Il file viene spostato in quarantena.

I file in quarantena possono essere scansionati con Avira Scanner (vedere capitolo: Quarantena: trattamento dei file (*.qua) in quarantena).

4.3.14 Profilo di ricerca: Inserire o eliminare un tipo di file in un profilo di ricerca

Per stabilire per un profilo di ricerca i tipi di file da scansionare o i tipi di file che devono essere esclusi dalla ricerca (possibile solo con selezione manuale e profili di ricerca personalizzati in questo modo):

- ✓ Da Control Center, selezionare la rubrica *SICUREZZA DEL COMPUTER* **> Scanner**.
- Fare clic con il tasto destro del mouse sul profilo di ricerca che si desidera modificare.
  - ↳ Verrà visualizzato un menu contestuale.
- Selezionare la voce **Filtro file**.
- Aprire nuovamente il menu contestuale facendo clic sul piccolo triangolo sul lato destro del menu contestuale.
  - ↳ Verranno visualizzate le voci **Standard**, **Scansiona tutti i file** e **Personalizzato**.
- Selezionare la voce **Personalizzato**.
  - ↳ Verrà visualizzata la finestra di dialogo **Estensioni file** con un elenco di tutti i tipi di file che devono essere abbinati al profilo di ricerca.

Se si desidera escludere un tipo di file dalla scansione:

- Selezionare il tipo di file e fare clic su **Elimina**.

Se si desidera aggiungere un tipo di file dalla scansione:

- Selezionare un tipo di file.
- Fare clic su **Aggiungi** e inserire l'estensione del tipo di file nel campo.

  Utilizzare un massimo di 10 caratteri e non inserire punti. I caratteri jolly * e ? sono ammessi.

4.3.15 Profilo di ricerca: creazione di un collegamento sul desktop per il profilo di scansione

Mediante un collegamento sul desktop a un profilo di scansione è possibile avviare una scansione diretta facendo clic sul desktop senza richiamare il Control Center del prodotto Avira in uso.

Per creare un collegamento al profilo di scansione dal desktop:

- ✓ Da Control Center, selezionare la rubrica *SICUREZZA DEL COMPUTER* **> Scanner**.
- Selezionare il profilo di scansione di cui si intende creare il collegamento.
- Fare clic sull'icona .
  - ↳ Viene creato un collegamento sul desktop.

4.3.16 Eventi: filtrare eventi

In Control Center, nel menu *AMMINISTRAZIONE* **> Eventi**, vengono visualizzati tutti gli eventi creati dai componenti del programma del prodotto Avira (analogamente alla visualizzazione eventi del sistema operativo Windows). I componenti del programma, in ordine alfabetico, sono i seguenti:

- Web Protection
- Real-Time Protection
- Mail Protection
- Servizio di assistenza
- Pianificatore
- Safe Browsing
- Scanner
- Updater
- ProActiv

Vengono visualizzati i seguenti tipi di eventi:

- *Informazione*
- *Avviso*
- *Errore*
- *Rilevamento*

Come filtrare gli eventi visualizzati:

- In Control Center selezionare la rubrica *AMMINISTRAZIONE* **> Eventi**.
- Attivare la casella di controllo dei componenti di programma per visualizzare gli eventi dei componenti attivi.

  \- OPPURE -

  Disattivare la casella di controllo dei componenti di programma per non visualizzare gli eventi dei componenti disattivati.
- Attivare la casella di controllo dei tipi di evento per visualizzare questi eventi.

  \- OPPURE -

  Disattivare la casella di controllo dei tipi di evento per non visualizzare questi eventi.

4.3.17 Mail Protection: esclusione degli indirizzi e-mail dalla scansione

Nel modo seguente è possibile impostare quali indirizzi e-mail (mittente) devono essere esclusi dalla scansione di Mail Protection (cosiddetta white list):

- Selezionare la rubrica *SICUREZZA INTERNET* **> Mail Protection** in Control Center.

↳ Nell'elenco vengono visualizzate le e-mail in ingresso.

- Selezionare l'e-mail che si desidera escludere dal controllo di Mail Protection.
- Fare clic sull'icona desiderata per escludere le e-mail dal controllo di Mail Protection:

L'indirizzo e-mail selezionato non verrà più scansionato in cerca di virus e programmi indesiderati.

↳ L'indirizzo e-mail del mittente verrà inserito nell'elenco delle eccezioni e non verrà più verificato in cerca di virus, malware.

Avviso
Escludere solo indirizzi e-mail di mittenti assolutamente attendibili dal controllo di Mail Protection.

Nota
Nella Configurazione in Mail Protection > Generale > Eccezioni è possibile inserire nell'elenco degli indirizzi da escludere altri indirizzi e-mail o eliminarne alcuni.

5. Rilevamento

5.1 Panoramica

In caso di rilevamento virus, il prodotto Avira può eseguire automaticamente determinate azioni o reagire in modo interattivo. In modalità di azione interattiva, in caso di rilevamento virus si apre una finestra di dialogo in cui è possibile gestire o avviare l'ulteriore trattamento del virus (cancellandolo, ignorandolo ecc.). In modalità automatica, è disponibile un'opzione che consente di visualizzare un avviso in caso di rilevamento di virus. Nel messaggio viene visualizzata l'azione che è stata eseguita automaticamente.

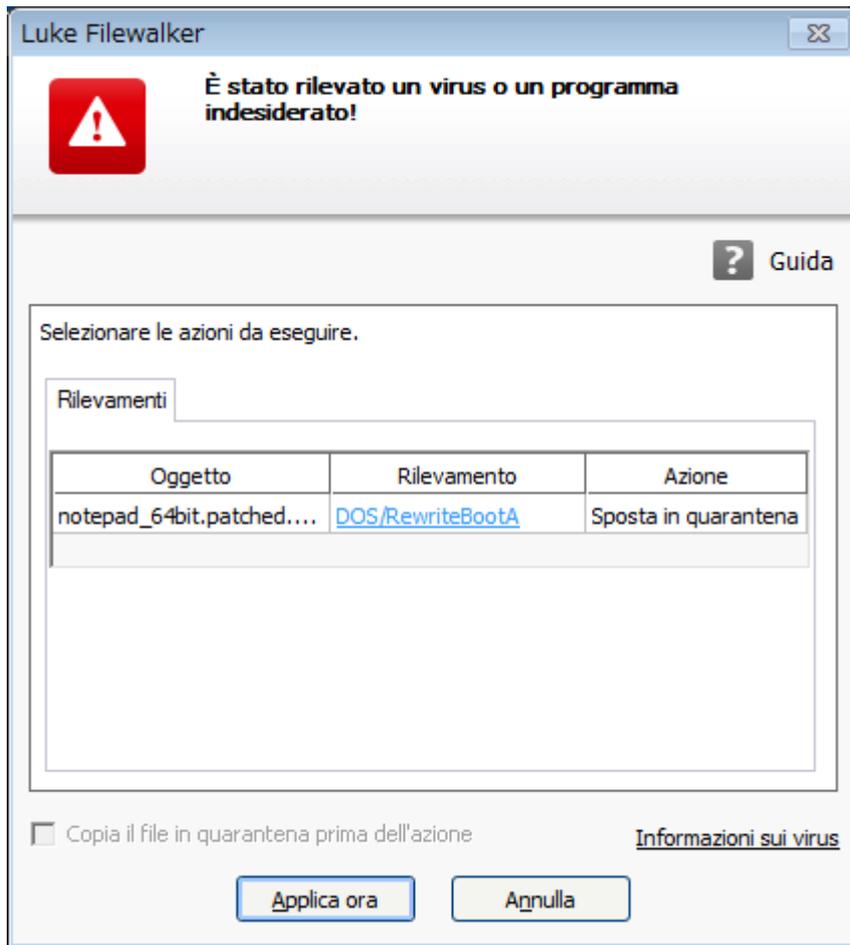
In questo capitolo è possibile ottenere tutte le informazioni sulle comunicazioni di un rilevamento ordinate per moduli.

- Vedere il capitolo Scanner: modalità di azione interattiva
- Vedere il capitolo Scanner: invio di file a Protection Cloud
- Vedere il capitolo Real-Time Protection
- Vedere il capitolo Real-Time Protection: Comportamento sospetto
- Vedere il capitolo Mail Protection: E-mail in ingresso
- Vedere il capitolo Mail Protection: E-mail in uscita
- Vedere il capitolo Invio di e-mail: Server
- Vedere il capitolo Invio di e-mail: Mittente
- Vedere il capitolo Web Protection

5.2 Modalità di azione interattiva

Durante la scansione dei file da parte di Scanner, al termine della scansione viene visualizzato un avviso con un elenco dei file infetti rilevati se come modalità di azione per il rilevamento virus è stata selezionata la modalità *interattiva* (vedere la rubrica di configurazione Scanner > Scansione > Azione in caso di rilevamento).
Mediante il menu contestuale è possibile selezionare un'azione da eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure chiudere Scanner.

> **Nota**
> Se la funzione di log è attivata Scanner riporta ogni rilevamento nel file di report.

5.2.1 Avviso

5.2.2 Rilevamenti, errori, avvisi

Nelle schede **Rilevamenti**, **Errori** e **Avvisi** vengono visualizzate le informazioni dettagliate e le opzioni di azione sui rilevamenti di virus e gli avvisi:

- **Rilevamenti:**
  - *Oggetto:* nome del file infetto
  - *Rilevamenti:* nome del virus o del programma indesiderato rilevato
  - *Azione:* azione selezionata per il trattamento del file infetto
    Nel menu contestuale dell'azione selezionata è possibile scegliere altre azioni per il trattamento di malware.
- **Errori:** messaggi di errori verificatisi durante la scansione
- **Avvisi:** avvisi riguardanti rilevamenti di virus

> **Nota**
> Nel tooltip sull'oggetto vengono visualizzate le seguenti informazioni: nome del

file infetto e percorso completo, nome del virus, azione eseguita con il pulsante **Applica ora**.

Nota
Come azione da eseguire, viene visualizzata per default l'azione standard di Scanner. L'azione standard di Scanner per il trattamento dei file infetti consiste nello spostamento in quarantena di questi ultimi.

5.2.3 Menu contestuale azioni

Nota
Se un rilevamento riguarda un oggetto euristico (HEUR/), un programma zip runtime insolito (PCK/) o un file con un'estensione occulta (HEUR-DBLEXT/), sono disponibili in modalità interattiva solo le opzioni Sposta in quarantena e Ignora. In modalità automatica, il rilevamento viene spostato automaticamente in quarantena.
Questa limitazione evita che i file per cui è stato emesso un falso allarme siano eliminati direttamente dal computer. Il file può essere ripristinato in ogni momento con l'aiuto del Gestore della quarantena.

Ripara

Se l'opzione è attivata, Scanner ripara il file infetto.

Nota
L'opzione **Ripara** è attivabile solo se è possibile eseguire una riparazione del file rilevato.

Quarantena

Se l'opzione è attivata, Scanner sposta il file in quarantena. Il file può essere ripristinato dal Gestore della quarantena se ha un valore informativo oppure, se necessario, inviato ad Avira Malware Research Center. A seconda del file sono disponibili altre possibilità di scelta nel Gestore della quarantena.

Elimina

Se l'opzione è attivata, il file viene eliminato. Questa procedura è molto più rapida di "Sovrascrivi ed elimina".

Sovrascrivi ed elimina

Se l'opzione è attivata, Scanner sovrascrive il file con un modello standard, infine lo elimina. Il file non può essere ripristinato.

Rinomina

Se l'opzione è attivata, Scanner rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). Il file può essere successivamente riparato e nuovamente rinominato.

Ignora

Se l'opzione è attivata, il file viene mantenuto.

Ignora sempre

Opzione di azione in caso di rilevamento di Real-Time Protection: Real-Time Protection non esegue nessun'altra azione. L'accesso al file è consentito. Tutti gli ulteriori accessi a questo file sono consentiti e non vengono più segnalati fino al riavvio del computer o all'aggiornamento del file di definizione dei virus.

Attenzione
Se si seleziona Ignora opzioni o Ignora sempre, i file infetti rimangono attivi sul computer. Questo potrebbe causare danni notevoli al computer.

5.2.4 Caratteristiche particolari nei rilevamenti di record di avvio infetti, rootkit e malware attivi

In caso di rilevamento di record di avvio infetti sono disponibili opzioni di azione per la riparazione:

722 KB | 1,44 MB | 2,88 MB | 360 KB | 1,2 MB Ripara record di avvio

Sono disponibili queste opzioni in caso di floppy disk infetti.

Scarica CD di ripristino

Mediante questa opzione si accede al sito Web Avira dove è possibile scaricare uno strumento speciale che riconosce e rimuove i virus del record di avvio.

Se si applicano azioni su processi in corso, i processi interessati vengono terminati prima dell'esecuzione dell'azione.

5.2.5 Pulsanti e link

Pulsante/Link	Descrizione
Applica ora	Le azioni selezionate vengono eseguite per il trattamento di tutti i file infetti.
Annulla	Scanner viene chiuso senza ulteriori azioni. I file infetti vengono lasciati sul computer.
Guida in linea	Con questo pulsante o link viene aperta questa pagina della guida in linea.

Attenzione
Eseguire l'azione *Annulla* solo in casi eccezionali e fondati. In caso di interruzione, i file infetti rimangono attivi sul computer. Questo potrebbe causare danni notevoli al computer.

5.2.6 Caratteristiche particolari nei rilevamenti in caso di Web Protection disattivato

Se Web Protection è stato disattivato, con un messaggio a tendina Real-Time Protection segnala il malware attivo rilevato durante la scansione del sistema. Prima di una riparazione è possibile creare un punto di ripristino del sistema.

✓ La funzione di ripristino del sistema deve essere attivata all'interno del sistema operativo Windows.

- Nel messaggio a tendina fare clic su **Visualizza dettagli**.
  ↪ Verrà visualizzata la finestra *Verifica del sistema in corso*.
- Attivare **Crea un punto di ripristino del sistema prima della riparazione**.
- Fare clic su **Applica**.
  ↪ È stato creato un punto di ripristino del sistema. A questo punto, è possibile effettuare un ripristino del sistema tramite il sistema operativo Windows.

5.3 Invio di file a Protection Cloud

Durante ogni **scansione rapida del sistema**, viene creato un elenco dei percorsi dei file che i programmi di malware utilizzano come destinazione. Nell'elenco sono contenuti, ad esempio, i processi in corso, le utility e i programmi di esecuzione automatica in uso. I file di programma sconosciuti saranno caricati per l'analisi del sistema Protection Cloud.

Se durante l'installazione personalizzata oppure durante la configurazione della **protezione avanzata** è stata attivata l'opzione **Conferma manuale in caso di invio di file sospetti ad Avira**, è possibile controllare l'elenco dei file sospetti e scegliere manualmente i file che si desidera caricare su Protection Cloud. Per impostazione predefinita, tutti i file sospetti vengono contrassegnati per essere caricati.

> **Nota**
> Se durante la configurazione di Scanner è stata attivata la funzione di log **estesa**, il file di report specifica un suffisso *(cloud)* per identificare gli avvisi del componente Protection Cloud.

5.3.1 Informazioni visualizzate

L'elenco dei file sospetti da caricare in Protection Cloud.

- *Inviare?:* è possibile scegliere i file che si desidera caricare in Protection Cloud.
- *File:* nome del file sospetto.
- *Percorso:* percorso del file sospetto.

Inviare sempre i file automaticamente

Se questa opzione è attiva, dopo ogni **scansione rapida del sistema** i file sospetti vengono inviati automaticamente all'analisi di Protection Cloud, senza necessità di alcuna conferma manuale.

5.3.2 Pulsanti e link

Pulsante/Link	Descrizione
Invia	I file selezionati vengono inviati ad Avira Protection Cloud.
Annulla	Scanner viene chiuso senza ulteriori azioni. I file infetti vengono lasciati sul computer.
Guida	Viene visualizzata questa pagina della guida in linea.
Informazioni su Protection Cloud	Viene visualizzata la pagina Web con informazioni su Protection Cloud.

Argomenti correlati:

- Configurazione della protezione avanzata
- Installazione personalizzata

- Configurazione report
- Visualizzazione report

5.4 Real-Time Protection

In caso di rilevamento virus da parte di Real-Time Protection, viene negato l'accesso al file e visualizzato un messaggio sul desktop se è stata selezionata come modalità di azione per il rilevamento virus la modalità *interattiva* (vedere la rubrica di configurazione Real-Time Protection > Scansione > Azione in caso di rilevamento).

Notifica

Nella notifica vengono visualizzate le seguenti informazioni:

- Data e ora del rilevamento
- Percorso e nome del file infetto
- Nome del malware

> **Nota**
> Al momento dell'avvio del computer, un'eventuale conseguenza della selezione della modalità di avvio di default per Real-Time Protection (avvio normale) e di un rapido accesso all'account utente può essere la mancata scansione dei programmi che si avviano automaticamente all'avvio del sistema, dal momento che essi vengono avviati prima del completo caricamento di Real-Time Protection.

Nella modalità interattiva sono disponibili le opzioni seguenti:

Rimuovi

Il file infetto viene trasmesso al componente **Scanner** e cancellato da questo. Non vengono visualizzati altri messaggi.

Dettagli

Il file infetto viene trasmesso al componente **Scanner**. Scanner segnala il rilevamento in una finestra, nella quale sono disponibili diverse opzioni per il trattamento del file infetto.

> **Nota**
> Prestare attenzione alle note riguardanti il trattamento del virus in Rilevamento > Scanner.

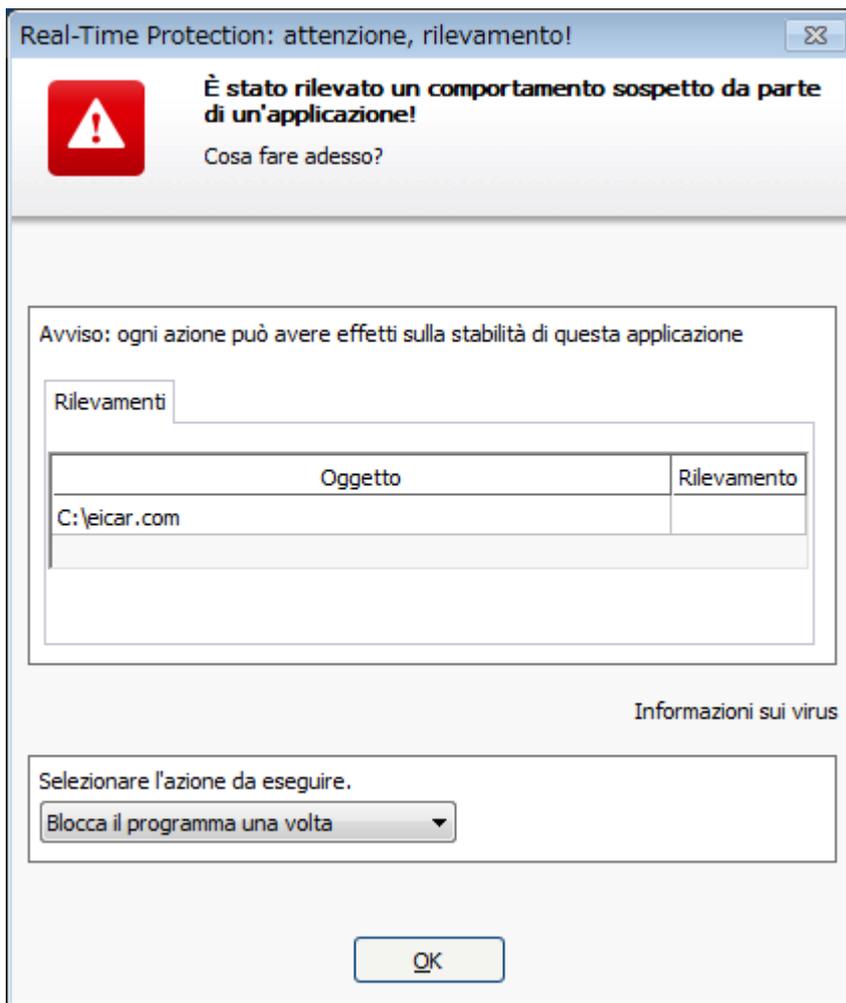
Nota
Nel messaggio di Scanner è preselezionata l'azione *Quarantena* indicata come azione standard. È possibile selezionare ulteriori azioni mediante il menu contestuale.

Chiudi

Il messaggio viene chiuso. Il trattamento del virus viene interrotto.

5.5 Comportamento sospetto

Se il componente ProActiv di Real-Time Protection viene attivato, vengono monitorate le azioni delle applicazioni e viene verificata la presenza di un comportamento sospetto tipico dei programmi di malware. Se viene rilevato un comportamento sospetto in un'applicazione, si riceve un avviso. Vi sono diverse opzioni per reagire al rilevamento.

5.5.1 Avviso di Real-Time Protection: È stato rilevato un comportamento sospetto da parte di un'applicazione

5.5.2 Nome e percorso del programma sospetto rilevato

Al centro della finestra del messaggio viene visualizzato il nome e il percorso dell'applicazione che esegue le azioni sospette.

5.5.3 Possibilità di scelta

Programma attendibile

Se l'opzione è attivata, l'esecuzione dell'applicazione prosegue. Il programma viene inserito nell'elenco delle applicazioni consentite ed escluso dal monitoraggio mediante il componente ProActiv. Aggiungendolo nell'elenco delle applicazioni consentite viene impostato il tipo di monitoraggio *Contenuti*. Questo significa che l'applicazione viene esclusa dal monitoraggio mediante il componente ProActiv solo in caso di contenuti non modificati (vedere Filtro di applicazione: Applicazioni consentite).

Blocca il programma una volta

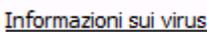
Se l'opzione è attivata, l'applicazione viene bloccata, quindi l'esecuzione dell'applicazione viene chiusa. Le azioni dell'applicazione continuano a essere monitorate dal componente ProActiv.

Blocca sempre questo programma

Se l'opzione è attivata, l'applicazione viene bloccata, quindi l'esecuzione dell'applicazione viene chiusa. Il programma viene inserito nell'elenco delle applicazioni da bloccare e non può più essere eseguito (vedere Filtro applicazione: applicazioni da bloccare).

Ignora

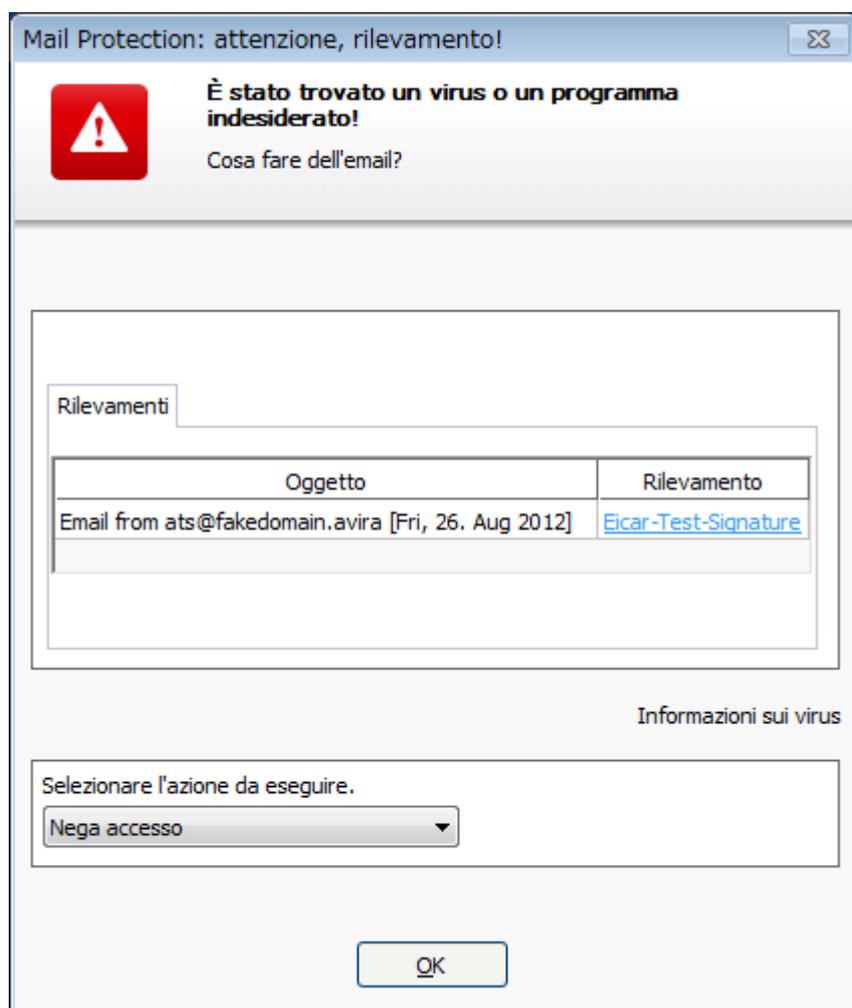
Se l'opzione è attivata, l'esecuzione dell'applicazione prosegue. Le azioni dell'applicazione continuano a essere monitorate dal componente ProActiv.

5.5.4 Pulsanti e link

Pulsante/Link	Descrizione
Informazioni sui virus	Grazie a questo link, se è presente un collegamento a Internet attivo, si accede alla pagina Internet per ottenere ulteriori informazioni su questo virus o programma indesiderato.
Guida in linea	Con questo pulsante o link viene aperta questa pagina della guida in linea.

5.6 E-mail in ingresso

In caso di rilevamento virus da parte di Mail Protection viene visualizzato un avviso se è stata selezionata come modalità di azione per il rilevamento virus la modalità *interattiva* (vedere la rubrica di configurazione Mail Protection > Scansione > Azione in caso di rilevamento). In modalità interattiva è possibile selezionare nella finestra di dialogo come procedere con l'e-mail o l'allegato.

L'avviso illustrato di seguito viene visualizzato quando il programma rileva un virus in un'e-mail in ingresso.

5.6.1 Avviso

5.6.2 Rilevamenti, errori, avvisi

Nelle schede **Rilevamenti**, **Errori** e **Avvisi** vengono visualizzati gli avvisi e le informazioni dettagliate sulle e-mail infette:

- **Rilevamenti:** oggetto: e-mail infetta con l'indicazione del mittente e del momento in cui l'e-mail è stata inviata

Rilevamenti: nome del virus o del programma indesiderato rilevato

- **Errori:** messaggi di errori verificatisi durante la scansione effettuata da Mail Protection
- **Avvisi:** avvisi riguardanti oggetti infetti

5.6.3 Possibilità di scelta

> **Nota**
> Se un rilevamento riguarda un oggetto euristico (HEUR/), un programma zip runtime insolito (PCK/) o un file con un'estensione occulta (HEUR-DBLEXT/), sono disponibili in modalità interattiva solo le opzioni Sposta in quarantena e Ignora. In modalità automatica, il rilevamento viene spostato automaticamente in quarantena.
> Questa limitazione evita che i file per cui è stato emesso un falso allarme siano eliminati direttamente dal computer. Il file può essere ripristinato in ogni momento con l'aiuto del Gestore della quarantena.

Sposta in quarantena

Se l'opzione è attivata, l'e-mail viene spostata con tutti gli allegati in quarantena. L'e-mail potrà essere inoltrata successivamente con il Gestore della quarantena. L'e-mail infetta viene eliminata. Il corpo del testo delle e-mail e gli eventuali allegati vengono sostituiti da un testo standard.

Elimina e-mail

Se l'opzione è attivata, l'e-mail infetta viene eliminata in caso di rilevamento di un virus o di un programma indesiderato. Il corpo del testo e gli eventuali allegati delle e-mail vengono sostituiti da un testo standard.

Elimina allegato

Se l'opzione è attivata, l'allegato infetto viene sostituito con un testo standard. Se il corpo del testo dell'e-mail risulta infetto, viene eliminato ed eventualmente sostituito da un testo standard. L'e-mail stessa viene inoltrata.

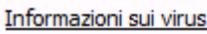
Sposta allegato in quarantena

Se l'opzione è attivata, l'allegato infetto viene collocato in quarantena e infine eliminato (sostituito con un testo standard). Il corpo dell'e-mail viene inoltrato. L'allegato infetto potrà essere successivamente inoltrato con il Gestore della quarantena.

Ignora

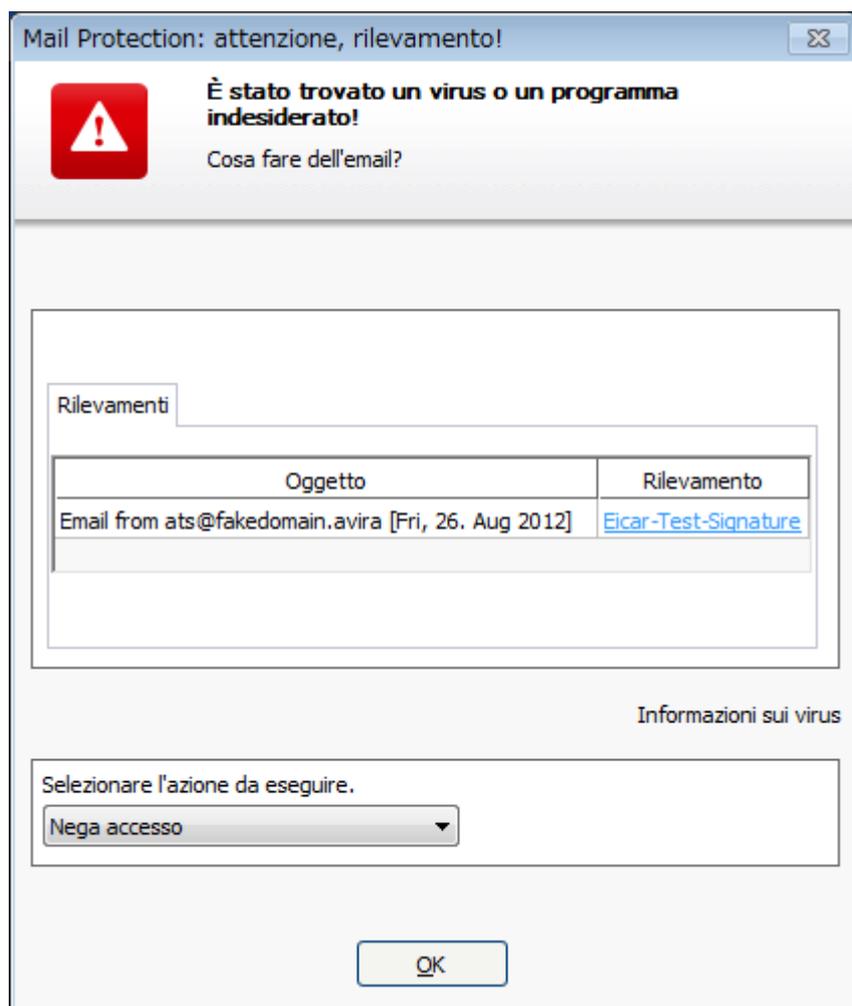
Se l'opzione è attivata, l'e-mail infetta viene inoltrata nonostante il rilevamento di un virus o di un programma indesiderato.

Avviso
In questo modo virus e programmi indesiderati potrebbero accedere al computer. Selezionare l'opzione **Ignora** solo in casi eccezionali e fondati. Disattivare l'anteprima in Microsoft Outlook, non aprire mai gli allegati facendo doppio clic!

5.6.4 Pulsanti e link

Pulsante/Link	Descrizione
Informazioni sui virus	Grazie a questo link, se è presente un collegamento a Internet attivo, si accede alla pagina Internet per ottenere ulteriori informazioni su questo virus o programma indesiderato.
Guida in linea	Con questo pulsante o link viene aperta questa pagina della guida in linea.

5.7 E-mail in uscita

In caso di rilevamento virus da parte di Mail Protection viene visualizzato un avviso se è stata selezionata come modalità di azione per il rilevamento virus la modalità *interattiva* (vedere la rubrica di configurazione Mail Protection > Scansione > Azione in caso di rilevamento). In modalità interattiva è possibile selezionare nella finestra di dialogo come procedere con l'e-mail o l'allegato.

5.7.1 Avviso

5.7.2 Rilevamenti, errori, avvisi

Nelle schede **Rilevamenti**, **Errori** e **Avvisi** vengono visualizzati gli avvisi e le informazioni dettagliate sulle e-mail infette:

- **Rilevamenti:** oggetto: e-mail infetta con l'indicazione del mittente e del momento in cui l'e-mail è stata inviata

  Rilevamenti: nome del virus o del programma indesiderato rilevato
- **Errori:** messaggi di errori verificatisi durante la scansione effettuata da Mail Protection
- **Avvisi:** avvisi riguardanti oggetti infetti

5.7.3 Possibilità di scelta

Sposta e-mail in quarantena (non inviare)

Se l'opzione è attivata, l'e-mail unitamente agli allegati viene copiata in quarantena e non inviata. L'e-mail resta nella Posta in uscita del client e-mail. Nel programma e-mail

viene visualizzato un messaggio di errore. In tutte le procedure di invio seguenti dell'account di posta elettronica questo messaggio viene verificato per malware.

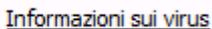
Blocca invio e-mail (non inviare)

L'e-mail non viene inviata e resta nella Posta in uscita del client e-mail. Nel programma e-mail viene visualizzato un messaggio di errore. In tutte le procedure di invio seguenti dell'account di posta elettronica questo messaggio viene verificato per malware.

Ignora

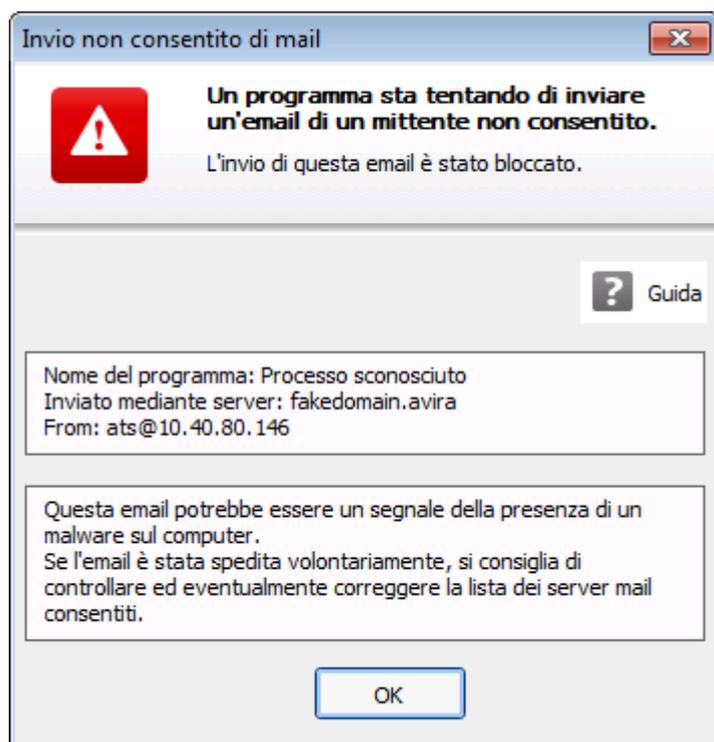
Se l'opzione è attivata, l'e-mail viene comunque inviata nonostante il rilevamento di un virus o di un programma indesiderato.

Avviso
In questo modo virus e programmi indesiderati potrebbero raggiungere il computer del destinatario dell'e-mail.

5.7.4 Pulsanti e link

Pulsante/Link	Descrizione
Informazioni sui virus	Grazie a questo link, se è presente un collegamento a Internet attivo, si accede alla pagina Internet per ottenere ulteriori informazioni su questo virus o programma indesiderato.
Guida in linea	Con questo pulsante o link viene aperta questa pagina della guida in linea.

5.8 Mittente

Se si utilizza la funzione AntiBot di Mail Protection, le e-mail di mittenti non autorizzati vengono bloccate da Mail Protection. Il controllo dei mittenti ha luogo in base all'elenco dei mittenti autorizzati registrati nella configurazione in Mail Protection > Scansione > AntiBot. L'e-mail bloccata viene segnalata in una finestra di dialogo.

5.8.1 Avviso

5.8.2 Programma utilizzato, server SMTP utilizzato e indirizzo del mittente dell'e-mail

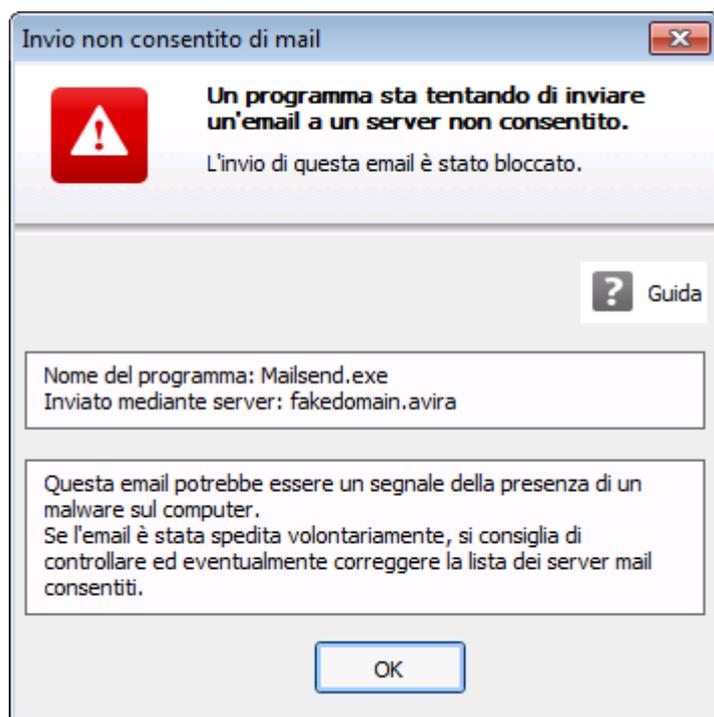
Al centro della finestra del messaggio vengono visualizzate le seguenti informazioni:

- Nome del programma utilizzato per l'invio dell'e-mail
- Nome del server SMTP utilizzato per l'invio dell'e-mail
- Indirizzo del mittente dell'e-mail

Se l'e-mail infetta è stata inviata mediante il programma di posta elettronica dell'utente, confrontare l'elenco dei mittenti autorizzati nella configurazione in Mail Protection > Scansione > AntiBot con gli indirizzi dei mittenti utilizzati negli account di posta elettronica del programma e-mail client. Se nella configurazione l'elenco dei mittenti autorizzati non è completo inserire gli altri indirizzi dei mittenti utilizzati. Le e-mail bloccate si trovano nella Posta in uscita del programma e-mail client. Per inviare le e-mail bloccate avviare nuovamente l'invio di e-mail dopo aver completato la configurazione.

5.9 Server

Se si utilizza la funzione AntiBot di Mail Protection, le e-mail inviate da server SMTP non autorizzati vengono bloccate da Mail Protection. Il controllo dei server SMTP utilizzati ha luogo in base all'elenco dei server autorizzati registrati nella configurazione in Mail Protection > Scansione > AntiBot. L'e-mail bloccata viene segnalata in una finestra di dialogo.

5.9.1 Avviso

5.9.2 Programma utilizzato, server SMTP utilizzato

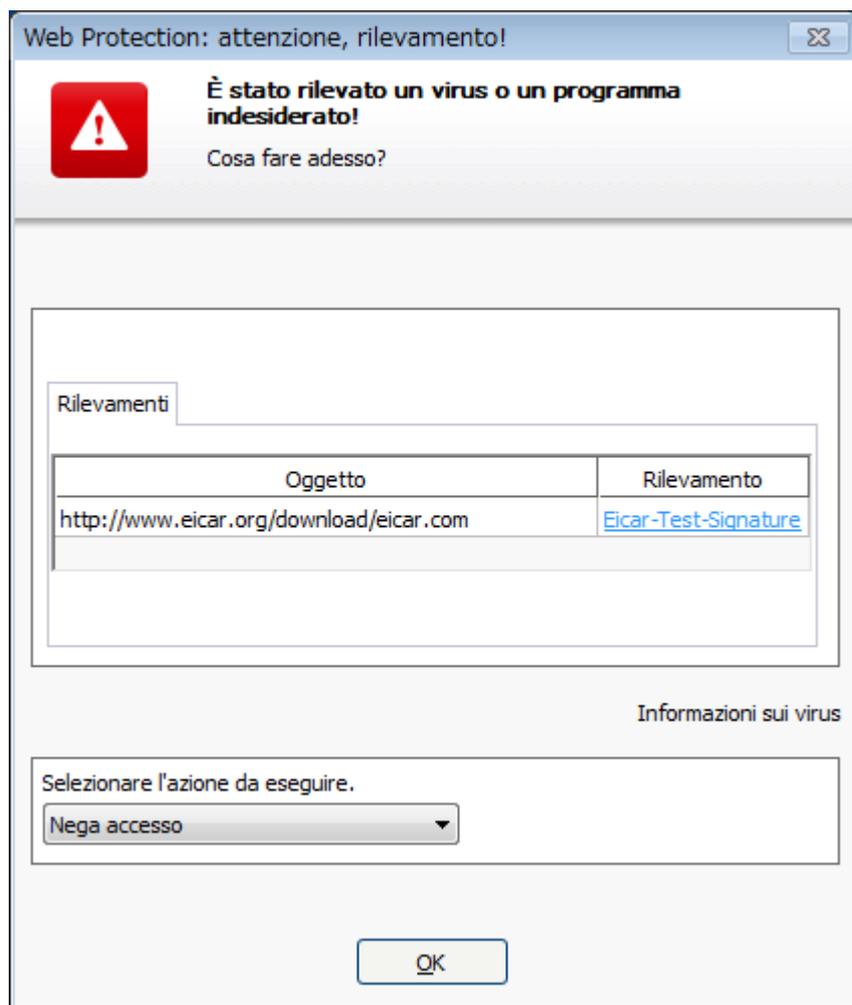
Al centro della finestra del messaggio vengono visualizzate le seguenti informazioni:

- Nome del programma utilizzato per l'invio dell'e-mail
- Nome del server SMTP utilizzato per l'invio dell'e-mail

Se l'e-mail infetta è stata inviata mediante il programma di posta elettronica dell'utente, confrontare l'elenco dei server autorizzati nella configurazione in Mail Protection > Scansione > AntiBot con i server SMTP utilizzati per inviare e-mail. Tali server SMTP possono essere richiamati nel programma client e-mail negli account di posta elettronica impiegati. Se nella configurazione l'elenco dei server autorizzati non è completo inserire gli altri server SMTP utilizzati. Le e-mail bloccate si trovano nella Posta in uscita del programma e-mail client. Per inviare le e-mail bloccate avviare nuovamente l'invio di e-mail dopo aver completato la configurazione.

5.10 Web Protection

In caso di rilevamento virus da parte di Web Protection, viene visualizzato un avviso se è stata selezionata come modalità di azione per il rilevamento virus la modalità *interattiva* (vedere la rubrica di configurazione Web Protection > Scansione > Azione in caso di rilevamento). In modalità interattiva è possibile selezionare nella finestra di dialogo come procedere con i dati trasferiti dal server Web.

Avviso

Rilevamenti, errori, avvisi

Nelle schede **Rilevamenti**, **Errori** e **Avvisi** vengono visualizzati gli avvisi e le informazioni dettagliate sui rilevamenti di virus:

- **Rilevamenti:** URL e nome del virus o del programma indesiderato rilevato
- **Errori:** messaggi di errori verificatisi durante la scansione effettuata da Web Protection
- **Avvisi:** avvisi riguardanti rilevamenti di virus

Azioni possibili

> **Nota**
> Se un rilevamento riguarda un oggetto euristico (HEUR/), un programma zip runtime insolito (PCK/) o un file con un'estensione occulta (HEUR-DBLEXT/), sono disponibili in modalità interattiva solo le opzioni Sposta in quarantena e Ignora.
> Questa limitazione evita che i file per cui è stato emesso un falso allarme siano

eliminati direttamente dal computer. Il file può essere ripristinato in ogni momento con l'aiuto del Gestore della quarantena.

Nega accesso

Il sito Web richiesto dal server Web o i dati e i file trasferiti non vengono inviati al proprio browser Web. Nel browser Web viene visualizzato un messaggio di errore relativo al divieto di accesso. Web Protection inserisce il rilevamento nel file di report, a condizione che la funzione di report sia attivata.

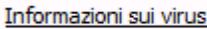
Isolamento (Sposta in quarantena)

Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inviati in quarantena in caso di rilevamento di un virus o di malware. Il file infetto può essere ripristinato dal Gestore della quarantena se ha un valore informativo, oppure, se necessario, inviato ad Avira Malware Research Center.

Ignora

Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inoltrati da Web Protection al proprio browser Web.

Avviso
In questo modo virus e programmi indesiderati potrebbero accedere al computer. Selezionare l'opzione **Ignora** solo in casi eccezionali e fondati.

Pulsanti e link

Pulsante/Link	Descrizione
Informazioni sui virus	Grazie a questo link, se è presente un collegamento a Internet attivo, si accede alla pagina Internet per ottenere ulteriori informazioni su questo virus o programma indesiderato.
Guida in linea	Con questo pulsante o link viene aperta questa pagina della guida in linea.

6. Scanner

6.1 Scanner

Con il componente Scanner è possibile effettuare scansioni mirate per virus e programmi indesiderati (scansione diretta). È possibile effettuare una scansione per file infetti in diversi modi:

- **Scansione diretta mediante il menu contestuale**
  La scansione diretta mediante il menu contestuale (tasto destro del mouse - voce **Controlla i file selezionati con Avira**) si consiglia quando, ad esempio, si desidera controllare singoli file e directory in Esplora risorse di Windows. Un ulteriore vantaggio è che Control Center non deve essere avviato per la scansione diretta mediante il menu contestuale.
- **Scansione diretta mediante Drag&Drop**
  Trascinando un file o una directory nella finestra di programma del Control Center, Scanner verifica il file o la directory, nonché tutte le sottodirectory. Questa procedura è consigliata quando si desidera controllare i singoli file e directory che sono stati archiviati, ad esempio, sul desktop.
- **Scansione diretta per profili**
  Questa procedura è consigliata quando si desidera controllare regolarmente alcune directory e drive (ad esempio la propria directory di lavoro o drive, sui quali si archiviano regolarmente nuovi file). Queste directory e drive non devono quindi essere selezionati a ogni scansione ma vengono comodamente selezionati tramite il profilo corrispondente.
- **Scansione diretta con il Pianificatore**
  Il Pianificatore offre la possibilità di far eseguire job temporizzati di scansione.

Durante la scansione per rootkit, virus del record di avvio e la scansione dei processi attivi sono necessari dei procedimenti particolari. Sono disponibili le seguenti opzioni:

- Scansione di rootkit mediante il profilo di ricerca **Scansione alla ricerca di rootkit e malware attivi**
- Scansione dei processi attivi mediante il profilo di ricerca **Processi attivi**
- Scansiona virus del record di avvio con il comando **Scansiona virus del record di avvio** nel menu **Extra**

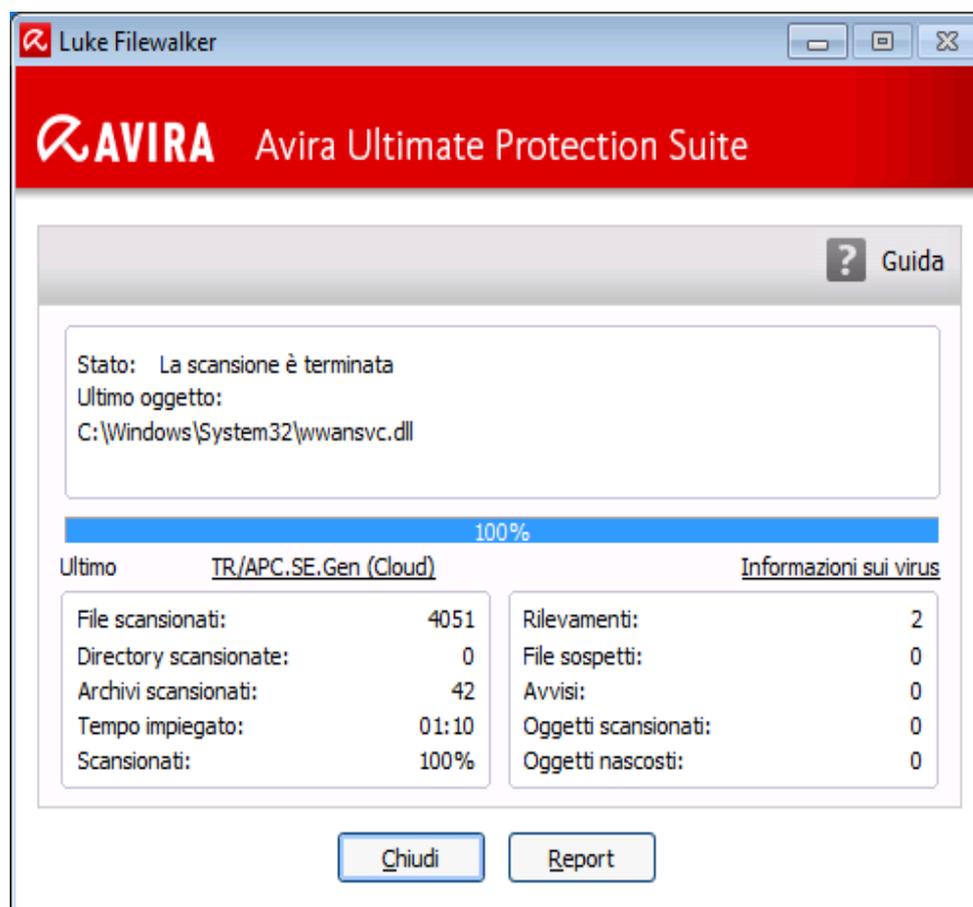
6.2 Luke Filewalker

Durante la scansione diretta appare la finestra sullo stato di **Luke Filewalker** che informa l'utente sullo stato della scansione.

Se nella configurazione di Scanner nel gruppo **Azione in caso di rilevamento** si seleziona l'opzione **interattivo**, in caso di rilevamento di un virus o di un programma

indesiderato viene chiesto all'utente come proseguire. Se è stata selezionata l'opzione **automatico**, in Report di Scanner saranno visibili gli eventuali rilevamenti.

Una volta conclusa la ricerca, i risultati della scansione (statistiche), gli avvisi e notifiche di errore vengono visualizzati in una finestra di dialogo successiva.

6.2.1 Luke Filewalker: finestra di stato della scansione

Informazioni visualizzate

Stato: Sono presenti diversi tipi di messaggio sullo stato:

- *Il programma viene inizializzato*
- *Si stanno cercando oggetti nascosti!*
- *Scansione dei processi avviati*
- *Scansione del file in corso*
- *Inizializzazione dell'archivio*
- *Libera memoria*
- *Decompressione del file*
- *Scansione dei record di avvio in corso*

- *Scansione dei record master di avvio in corso*
- *Scansione del registro in corso*
- *Il programma viene chiuso!*
- *La scansione è terminata*

Ultimo oggetto: nome e percorso del file che viene scansionato o è stato scansionato recentemente

Ultimo rilevamento: sono presenti diversi tipi di messaggio sull'ultimo rilevamento:

- *Nessun virus rilevato.*
- Nome dell'ultimo virus o del programma indesiderato rilevato

File scansionati: numero di file scansionati

Directory scansionate: numero di directory scansionate

Archivi scansionati: numero degli archivi scansionati

Tempo impiegato: durata della scansione diretta

Scansionati: quota percentuale della scansione già eseguita

Rilevamenti: numero di virus o programmi indesiderati rilevati

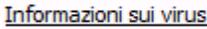
File sospetti: numero dei file segnalati dall'euristica

Avvisi: numero degli avvisi di rilevamento di virus

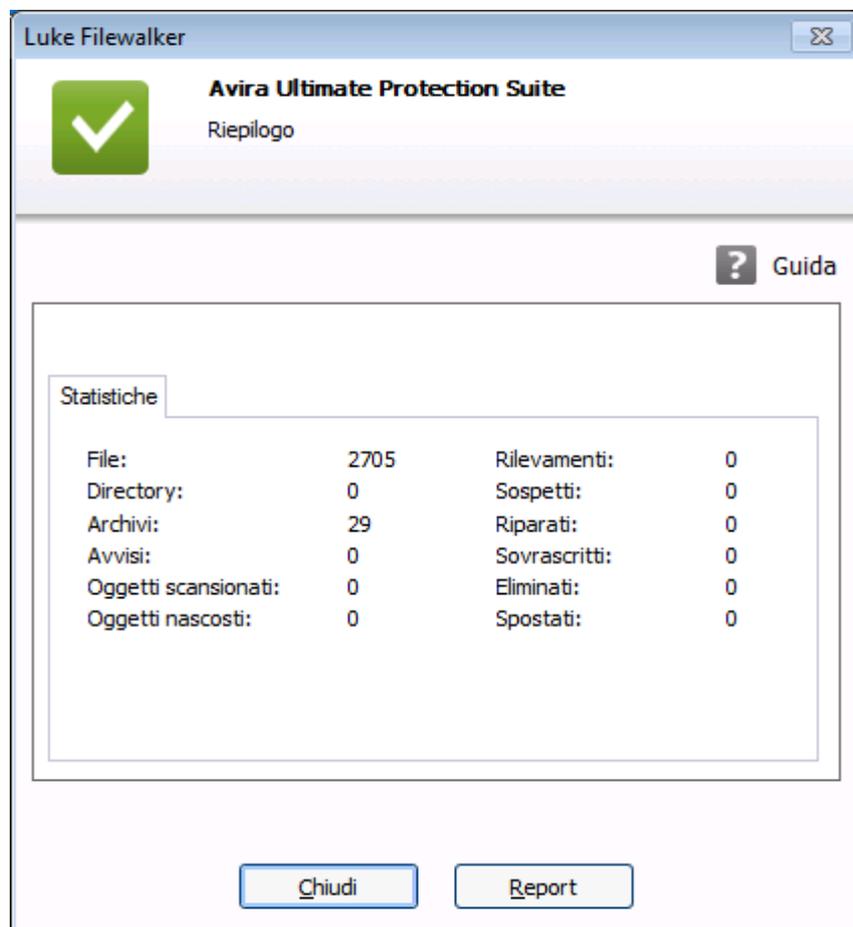
Oggetti scansionati: numero di oggetti analizzati dalla ricerca dei rootkit

Oggetti nascosti: numero complessivo degli oggetti nascosti trovati

Nota
I rootkit hanno la capacità di nascondere processi e oggetti, ad esempio voci di registro o file, ma non tutti gli oggetti nascosti sono necessariamente indicatori dell'esistenza di un rootkit. Gli oggetti nascosti possono anche essere oggetti innocui. Se durante la scansione vengono trovati oggetti nascosti ma non viene visualizzato nessun messaggio d'avviso indicante il rilevamento di virus, in base al report occorre stabilire di quali oggetti si tratta e recuperare maggiori informazioni sugli oggetti trovati.

Pulsanti e link

Pulsante/Link	Descrizione
Informazioni sui virus	Grazie a questo link, se è presente un collegamento a Internet attivo, si accede alla pagina Internet per ottenere ulteriori informazioni su questo virus o programma indesiderato.
Guida in linea	Apre questa pagina della guida in linea.
Stop	La scansione verrà terminata.
Pausa	La scansione viene interrotta e può essere ripresa con il pulsante **Prosegui**.
Prosegui	La scansione interrotta viene ripresa.
Chiudi	Scanner viene chiuso.

Report	Viene visualizzato il file di report della scansione.

6.2.2 Luke Filewalker: statistiche della scansione

Informazioni visualizzate: statistiche

File: numero dei file scansionati

Directory: numero delle directory scansionate

Archivio: numero degli archivi scansionati

Avvisi: numero degli avvisi di rilevamento di virus

Oggetti scansionati: numero di oggetti analizzati dalla ricerca dei rootkit

Oggetti nascosti: numero degli oggetti nascosti rilevati (rootkit)

Rilevamenti: numero di virus o programmi indesiderati rilevati

Sospetti: numero dei file segnalati dall'euristica

Riparati: numero dei file riparati

Sovrascritti: numero dei file sovrascritti

Eliminati: numero dei file eliminati

Spostati: numero dei file spostati in quarantena

Pulsanti e link

Pulsante/Link	Descrizione
Guida in linea	Apre questa pagina della guida in linea.
Chiudi	La finestra di riepilogo viene chiusa.
Report	Viene visualizzato il file di report della scansione.

7. Control Center

7.1 Panoramica

Il Control Center funge da centro informazioni, configurazione e gestione. Oltre alle Rubriche selezionabili singolarmente, sono disponibili numerose opzioni, raggiungibili tramite la barra dei menu.

Barra dei menu

Nella barra dei menu sono disponibili le seguenti funzioni:

File

- Esci (Alt+F4)

Visualizza

- Stato
- Sicurezza del computer
  - System Scanner
  - Real-Time Protection
- Sicurezza Internet
  - FireWall
  - Web Protection
  - Mail Protection
- Protezione dei bambini
  - Safe Browsing
- Protezione mobile
  - Avira Free Android Security
- Amministrazione
  - Quarantena
  - Pianificatore
  - Report
  - Eventi
- Aggiorna (F5)

Extra

- Scansione dei record di avvio...
- Elenco rilevamento...

- Scarica CD di ripristino
- Configurazione (F8)

Aggiornamento

- Avvia l'aggiornamento...
- Aggiornamento manuale...

Aiuto

- Argomenti
- Aiutami
- Supporto live
- Forum
- Scarica manuale
- Gestione delle licenze
- Consiglia prodotto
- Invia feedback
- Informazioni su Avira Ultimate Protection Suite

> **Nota**
> Attivare la navigazione da tastiera nella barra dei menu con l'ausilio del tasto [**Alt**]. Se la navigazione con tastiera è attivata, è possibile spostarsi all'interno dei menu con i tasti freccia. Con il tasto Invio si attiva la voce di menu selezionata in quel momento.

Rubriche

Nella barra di navigazione a sinistra sono presenti le seguenti rubriche:

- Stato

SICUREZZA DEL COMPUTER

- System Scanner
- Real-Time Protection

SICUREZZA INTERNET

- FireWall
- Web Protection
- Mail Protection

PROTEZIONE DEI BAMBINI

- Safe Browsing

PROTEZIONE MOBILE

- Avira Free Android Security

AMMINISTRAZIONE

- Quarantena
- Pianificatore
- Report
- Eventi

Descrizione delle rubriche

- **Stato**: nella schermata iniziale **Stato** sono presenti tutte le rubriche per controllare le funzionalità del programma (vedere Stato).
  - La finestra **Stato** offre la possibilità di visualizzare quali moduli sono attivi e fornisce informazioni sull'ultimo aggiornamento effettuato.
- *SICUREZZA DEL COMPUTER*: in questa rubrica sono disponibili i componenti con cui eseguire la scansione di virus e malware nei file del computer.
  - La rubrica **System Scanner** offre la possibilità di configurare o avviare la scansione diretta in modo semplice (vedere System Scanner). I profili predefiniti consentono di eseguire una scansione con le opzioni standard già adeguate. Con l'aiuto della Selezione manuale (viene memorizzata) o con la creazione di Profili personalizzati, è possibile adattare la scansione di virus e programmi indesiderati alle proprie esigenze personali.
  - La rubrica Real-Time Protection mostra le informazioni sui file scansionati e altri dati statistici, che possono essere ripristinati in ogni momento e permette di richiamare il file di report. Informazioni dettagliate sull'ultimo virus o programma indesiderato trovato sono reperibili premendo un pulsante.
- *SICUREZZA INTERNET*: contiene i componenti che consentono di proteggere il computer da virus e malware provenienti da Internet, nonché da accessi di rete indesiderati.
  - Nella rubrica **FireWall** è possibile configurare le impostazioni di base Firewall. Vengono inoltre visualizzate le attuali velocità di trasferimento dati e tutte le applicazioni attive che utilizzano un collegamento alla rete (vedere FireWall).
  - La rubrica Web Protection visualizza informazioni sugli URL scansionati e sui virus individuati, nonché ulteriori dati statistici, che possono essere ripristinati in qualsiasi momento e consente di richiamare il file di report. Informazioni dettagliate sull'ultimo virus o programma indesiderato trovato sono reperibili premendo un pulsante.
  - La rubrica **Mail Protection** mostra le e-mail verificate, le loro proprietà e altri dati statistici. Inoltre, è possibile spostare escludere per il futuro indirizzi e-mail dalla

scansione per malware o spam. Le e-mail possono essere eliminate anche dalla memoria temporanea di Mail Protection. Vedere Mail Protection.

- *PROTEZIONE DEI BAMBINI*: contiene i tool per consentire ai bambini di navigare su Internet in sicurezza.
  - Safe Browsing: è possibile assegnare ruoli utente agli utenti del computer. Il ruolo utente può essere configurato e comprende un set di regole con i seguenti criteri: URL vietati e consentiti (indirizzi Internet), categorie di contenuti vietate, durata di permanenza su Internet ed eventualmente periodi di utilizzo consentiti per i giorni della settimana
- *PROTEZIONE MOBILE*: dalla categoria Avira Free Android Security è possibile accedere online ai dispositivi Android.
  - Avira Free Android Security consente di amministrare tutti i dispositivi basati sul sistema operativo Android.
- *AMMINISTRAZIONE*: contiene i tool per l'isolamento e l'amministrazione dei file sospetti o infetti e la pianificazione delle attività ricorrenti.
  - Nella rubrica **Quarantena** è disponibile il cosiddetto Gestore della quarantena, la postazione centrale per i file già in quarantena o per file sospetti che si desidera spostare in quarantena (vedere Quarantena). Inoltre esiste la possibilità di inviare un file selezionato per e-mail all'Avira Malware Research Center.
  - La rubrica **Pianificatore** consente di creare job temporizzati di controllo e di aggiornamento nonché di backup e di cancellare o modificare job esistenti (vedere Pianificatore).
  - La rubrica **Report** consente di visualizzare i risultati delle azioni eseguite (vedere Report).
  - La rubrica **Eventi** consente di ottenere informazioni sugli eventi generati dai moduli del programma (vedere Eventi).

Pulsanti e link

Sono disponibili i seguenti pulsanti e link.

Pulsante/Link	Collegamento	Descrizione
Configurazione		Viene richiamata la finestra di dialogo di configurazione della rubrica.
	F1	Viene visualizzato l'argomento corrispondente della Guida in linea.

7.2 File

7.2.1 Chiudi

La voce di menu **Chiudi** nel menu **File** chiude il Control Center.

7.3 Visualizza

7.3.1 Stato

La schermata iniziale di Control Center **Stato** consente di verificare immediatamente se il computer è protetto e quali moduli Avira sono attivi. Inoltre la finestra **Stato** fornisce informazioni sull'ultimo aggiornamento seguito. Inoltre, è possibile verificare se si possiede una licenza valida.

- Sicurezza PC: Real-Time Protection, Ultima scansione, Ultimo aggiornamento, Il vostro prodotto è attivo
- Sicurezza Internet: Web Protection, Mail Protection, FireWall, Safe Browsing, Modalità gioco,

> **Nota**
> La gestione account cliente (UAC) necessita del vostro consenso per l'attivazione o la disattivazione dei servizi di Real-Time Protection, FireWall, Web Protection e Mail Protection nei sistemi operativi a partire da Windows Vista.

Sicurezza del computer

In questa sezione vengono visualizzate informazioni sullo stato attuale dei servizi e delle funzioni di protezione che proteggono il computer da virus e malware.

Real-Time Protection

In questa sezione sono disponibili informazioni sullo stato attuale di Real-Time Protection.

È possibile attivare e disattivare Real-Time Protection tramite il pulsante **Attiva/Disattiva**. Per le altre opzioni di Real-Time Protection, fare clic sulla barra di navigazione **Real-Time Protection**. Verranno visualizzate le informazioni di stato sugli ultimi malware rilevati e file infetti. Fare clic su **Configurazione** per effettuare altre impostazioni.

- **Configurazione**: si accede alla configurazione dove è possibile effettuare le impostazioni per i componenti del modulo Real-Time Protection.

Sono disponibili le seguenti possibilità:

Icona	Stato	Opzione	Descrizione
	Attivato	**Disattiva**	Il servizio Real-Time Protection è attivo, pertanto il sistema viene costantemente monitorato per rilevare la presenza di virus o programmi indesiderati. **Nota** Il servizio Real-Time Protection può essere disattivato. Tenere presente però che disattivando Real-Time Protection il computer non sarà più protetto da virus e programmi indesiderati. Tutti i file possono penetrare indisturbati nel sistema e causare un danno.
	Disattivato	**Attiva**	Il servizio Real-Time Protection è disattivato, ovvero il servizio è caricato, ma non è attivo. **Avviso** Non verrà effettuata la ricerca di virus o programmi indesiderati. Tutti i file possono penetrare nel sistema indisturbati. Il sistema non è protetto da virus o programmi indesiderati. **Nota** Per ripristinare la protezione contro virus e programmi indesiderati, fare clic sul pulsante **Attiva/Disattiva** accanto a Real-Time Protection nel riquadro Sicurezza del computer della finestra di stato.

<table>
<tr><td rowspan="2"></td><td>Servizio arrestato</td><td>Avvia</td><td>Il servizio Real-Time Protection è stato arrestato.

Avviso
Non verrà effettuata la ricerca di virus o programmi indesiderati. Tutti i file possono penetrare nel sistema indisturbati. Il sistema non è protetto da virus o programmi indesiderati.

Nota
Per ripristinare la protezione contro virus e programmi indesiderati, fare clic sul pulsante Attiva/Disattiva. Ora lo stato attuale dovrebbe essere visualizzato come Attivato.</td></tr>
<tr><td>Sconosciuto</td><td>Aiuto</td><td>Questo stato viene visualizzato in caso di un errore sconosciuto. In questo caso rivolgersi al nostro Supporto.</td></tr>
</table>

Ultima scansione

In questa sezione sono disponibili informazioni sull'ultima scansione del sistema. Nella scansione completa del sistema sono inclusi tutti gli hard disk del computer. Durante la ricerca vengono eseguite tutte le procedure di scansione e di verifica, ad eccezione del controllo dell'integrità dei file di sistema: scansione standard di file, verifica del registro e dei record di avvio, ricerca di rootkit e malware attivi, ecc.

Vengono visualizzati:

- la data dell'ultima scansione completa

Sono disponibili le seguenti possibilità:

Scansione di sistema	Opzione	Descrizione
Non eseguito	**Analizza il sistema ora**	Dall'installazione non è stata eseguita ancora una scansione completa del sistema. **Avviso** Lo stato del sistema non è stato verificato. Esiste la possibilità che sul computer siano presenti virus e programmi indesiderati. **Nota** Per eseguire una scansione del computer, fare clic sul pulsante Analizza il sistema ora.
Data dell'ultima scansione del sistema, ad esempio *18/09/2011*	**Analizza il sistema ora**	È stata seguita una scansione completa del sistema nella data indicata. **Nota** Si consiglia di utilizzare il job di scansione standard *Scansione completa del sistema*: attivare il job di scansione Scansione completa del sistema nel Pianificatore.
Sconosciuto	**Aiuto**	Questo stato viene visualizzato in caso di un errore sconosciuto. In questo caso rivolgersi al nostro Supporto.

Ultimo aggiornamento

In questa sezione sono disponibili informazioni sullo stato attuale dell'ultimo aggiornamento effettuato.

Vengono visualizzati:

- la data dell'ultimo aggiornamento
  - Fare clic sul pulsante Configurazione per effettuare altre impostazioni di aggiornamento automatico.

Sono disponibili le seguenti possibilità:

Icona	Stato	Opzione	Descrizione
✅	Data dell'ultimo aggiornamento, ad esempio *18/07/2011*	**Avvia aggiornamento**	Il programma è stato aggiornato nelle ultime 24 ore. **Nota** Facendo clic sul pulsante Avvia aggiornamento è possibile aggiornare il prodotto Avira in uso allo stato più recente.
!	Data dell'ultimo aggiornamento, ad esempio *15/07/2011*	**Avvia aggiornamento**	Dall'aggiornamento sono già trascorse 24 ore, tuttavia è ancora attivo il ciclo di avvisi per ricordare di eseguire l'aggiornamento selezionato dall'utente. Ciò dipende dalle impostazioni nella configurazione. **Nota** Facendo clic sul pulsante Avvia aggiornamento è possibile aggiornare il prodotto Avira in uso allo stato più recente.

	Non eseguito	**Avvia aggiornamento**	Dall'installazione non è stato effettuato nessun aggiornamento oppure il ciclo di avvisi per ricordare di eseguire l'aggiornamento selezionato dall'utente è stato superato (vedere Configurazione) e non è stato eseguito nessun aggiornamento oppure il file di definizione dei virus è precedente al ciclo di avvisi per ricordare di eseguire l'aggiornamento selezionato dall'utente (vedere Configurazione). **Nota** Facendo clic sul pulsante **Avvia aggiornamento** il prodotto Avira in uso viene portato allo stato più recente.
		Non disponibile	In caso di licenza scaduta non è possibile effettuare aggiornamenti.

Il prodotto è attivo

In questa sezione sono disponibili informazioni sullo stato attuale della licenza.

Sono disponibili le seguenti possibilità:

Versione completa

Icona	Stato	Opzione	Significato
	Data di validità della licenza attuale per una versione completa, ad esempio *31/10/2011*	**Rinnova**	Siete in possesso di una licenza valida per il prodotto Avira. Facendo clic sul pulsante Rinnova, potete accedere al negozio online di Avira. Facendo clic sul pulsante Rinnova si accede al negozio online di Avira, in cui è possibile adeguare la licenza alle proprie esigenze ed eseguire un aggiornamento ad Avira Premium.
	Data di validità della licenza attuale per una versione completa, ad esempio *31/10/2011*	**Rinnova**	L'utente è in possesso di una licenza valida del prodotto Avira. Il periodo di licenza dura tuttavia appena 30 giorni o meno. Facendo clic sul pulsante **Rinnova**, l'utente accede al negozio online di Avira. Qui l'utente ha la possibilità di prolungare la propria licenza attuale.
	Licenza scaduta il: ad esempio il *31/08/2011*	**Acquista**	La licenza del prodotto Avira è scaduta. Facendo clic sul pulsante **Acquista**, l'utente accede al negozio online di Avira. Qui l'utente ha la possibilità di acquistare una licenza attuale. **Avviso** Se la licenza è scaduta, non è più possibile effettuare aggiornamenti. Le funzioni di protezione del programma sono disattivate e non è più possibile riattivarle.

Licenza di evaluation

Icona	Stato	Opzione	Significato
	Data di validità della licenza di evaluation, ad esempio *31/10/2011*	**Acquista**	L'utente è in possesso di una licenza di evaluation e ha la possibilità di provare il prodotto Avira per un periodo determinato in tutte le sue funzioni. Facendo clic sul pulsante **Acquista**, l'utente accede al negozio online di Avira. Qui l'utente ha la possibilità di acquistare una licenza attuale.
	Data di validità della licenza di evaluation, ad esempio *31/10/2011*	**Rinnova**	L'utente è in possesso di una licenza di evaluation. Il periodo di licenza dura tuttavia appena 30 giorni o meno. Facendo clic sul pulsante **Rinnova**, l'utente accede al negozio online di Avira. Qui l'utente ha la possibilità di acquistare una licenza attuale.
	Licenza di evaluation scaduta il: *31/08/2011*	**Acquista**	La licenza del prodotto Avira è scaduta. Facendo clic sul pulsante **Acquista**, l'utente accede al negozio online di Avira. Qui l'utente ha la possibilità di acquistare una licenza attuale. **Avviso** Se la licenza è scaduta, non è più possibile effettuare aggiornamenti. Le funzioni di protezione del programma sono disattivate e non è più possibile riattivarle.

Sicurezza Internet

In questa sezione vengono visualizzate informazioni sullo stato attuale dei servizi e delle funzioni di protezione che proteggono il computer da virus e malware provenienti da Internet.

- **FireWall**: questo servizio controlla le vie di comunicazione da e verso il computer.
- **Web Protection**: il servizio verifica i dati che vengono trasferiti navigando su Internet e caricati nei browser Web (monitoraggio delle porte 80, 8080, 3128).

- **Mail Protection**: il servizio verifica la presenza di virus e malware nelle e-mail e negli allegati.
- **Safe Browsing**: La funzione di protezione bambini basata sui ruoli filtra contenuti Web indesiderati e illegali, controlla e gestisce l'utilizzo di Internet a tempo.

> **Nota**
> **Safe Browsing** non è un vero e proprio servizio (processo), bensì una funzionalità di **Web Protection**.

- **Modalità gioco**: se quest'opzione è attiva, quando viene eseguita un'applicazione a schermo intero, il prodotto Avira passa automaticamente alla modalità gioco . Vedere Modalità gioco.

Ulteriori opzioni relative a questi servizi sono visualizzabili nel menu contestuale che compare facendo clic sul pulsante **Configurazione** accanto a **Attiva/Disattiva**:

- **Configurazione**: si accede alla configurazione dove è possibile effettuare le impostazioni per i componenti di questo servizio.

Sono disponibili le seguenti possibilità: *Servizi*

Icona	Stato	Stato del servizio	Opzione	Significato
✅	*OK*	Attivato	**Disattiva**	Tutti i servizi di Sicurezza Internet sono attivi. **Nota** Per disattivare un servizio, fare clic sul pulsante **Attiva/Disattiva**. Tenere presente però che, disattivando il servizio, il computer non sarà più protetto da virus e malware.

<table>
<tr>
<td>!</td>
<td>Limitato</td>
<td>Disattivato</td>
<td>Attiva</td>
<td>Il servizio è disattivato, ovvero il servizio è avviato ma non è attivo.

Avviso
Il computer non è monitorato completamente. Esiste la possibilità che penetrino virus e programmi indesiderati nel computer.

Nota
Per attivare il servizio, fare clic sul pulsante Attiva/Disattiva accanto al servizio corrispondente.</td>
</tr>
</table>

	Avviso	Servizio arrestato	**Avvia**	È stato arrestato un servizio. **Avviso** Il computer non è monitorato completamente. Esiste la possibilità che penetrino virus e programmi indesiderati nel computer. **Nota** Per avviare il servizio e lasciar monitorare il computer, fare clic sul pulsante **Attiva/Disattiva**. Il servizio verrà avviato e attivato.
		Sconosciuto	**Aiuto**	Questo stato viene visualizzato in caso di un errore sconosciuto. In questo caso rivolgersi al nostro Supporto.

Sono disponibili le seguenti possibilità: Safe Browsing

Icona	Stato	Stato funzionalità	Opzione	Significato
✅	*OK*	Attivato	**Configura**	**Web Protection** e la funzione **Safe Browsing** sono attivi. **Nota** Mediante il pulsante **Configurazione**, a destra della funzione **Safe Browsing**, si accede alla configurazione dove è possibile effettuare ulteriori impostazioni relative a Protezione dei bambini. Tenere presente che nei ruoli utente standard preconfigurati (bambino, adolescente e adulto), la funzione di monitoraggio e controllo a tempo dell'utilizzo di Internet è disattivata.

!	*Limitato*	Disattivato	**Configura**	**Safe Browsing** non è attivo. - OPPURE - Il servizio **Real-Time Protection** è stato disattivato. **Avviso** Se **Web Protection** è stato disattivato, il computer non è monitorato completamente. Esiste la possibilità che penetrino virus e programmi indesiderati nel computer. **Nota** Per attivare **Safe Browsing**, fare clic sul pulsante **Attiva/Disattiva**. Mediante il pulsante Configurazione si accederà alla configurazione, in cui è possibile effettuare ulteriori impostazioni relative a Protezione dei bambini.

7.3.2 Modalità di riproduzione

Se sul computer vengono eseguite applicazioni che richiedono la modalità a schermo intero, è possibile attivare la modalità di riproduzione per nascondere gli avvisi sul desktop e le comunicazioni come finestre di popup e messaggi sul prodotto.

È possibile attivare la modalità di riproduzione facendo clic sul pulsante **ATTIVA/DISATTIVA** oppure proseguire in modalità automatica. La modalità di riproduzione predefinita è **Automatica** e viene indicata in verde. Con quest'impostazione, quando viene eseguita un'applicazione a schermo intero, il prodotto Avira passa automaticamente alla modalità di riproduzione.

- Per attivare la modalità di riproduzione, fare clic sul pulsante a sinistra accanto al pulsante **DISATTIVA**.
  - ↳ La modalità di riproduzione è attiva e il pulsante è giallo.

> **Nota**
> Si consiglia di modificare soltanto temporaneamente lo stato predefinito **DISATTIVA** con il riconoscimento automatico delle applicazioni in modalità a schermo intero, perché nella modalità di riproduzione non vengono visualizzati i messaggi sul desktop, gli avvisi sugli accessi alla rete e gli eventuali rischi.

7.3.3 System Scanner

La rubrica **System Scanner** consente di configurare o avviare in modo semplice una scansione del sistema. I profili predefiniti consentono di eseguire una scansione con le opzioni standard già adeguate. Con l'aiuto della selezione manuale o con la creazione di profili personalizzati è possibile adattare la ricerca di virus e programmi indesiderati alle proprie esigenze personali. L'azione desiderata è raggiungibile mediante la selezione dell'icona nella barra degli strumenti, mediante collegamento o con il menu contestuale. È possibile avviare una scansione mediante la voce Avvia la scansione con il profilo selezionato.

La visualizzazione e la gestione dei profili editabili corrispondono a quelle di Esplora risorse di Windows. Ciascuna cartella nella directory principale corrisponde a un profilo. La cartella o i file da scansionare sono contrassegnati o possono essere contrassegnati con un segno di spunta davanti alla cartella o al file da scansionare.

- Per cambiare directory, fare doppio clic sulla directory desiderata.
- Per cambiare i drive, fare doppio clic sulla lettera del drive desiderato.
- Per selezionare cartelle e drive è possibile fare clic sulle caselle di spunta prima della cartella o drive, oppure effettuare la scelta nel menu contestuale.
- È possibile navigare nella struttura del menu con aiuto della barra di scorrimento e delle relative frecce.

Profilo predefinito

Per la scansione sono disponibili i profili predefiniti.

> **Nota**
> Tali profili sono protetti dalla scrittura e non possono essere modificati o eliminati. Per adattare un profilo alle proprie esigenze selezionare per un'unica scansione la cartella Selezione manuale o Crea nuovo profilo per la creazione di un profilo personalizzato che possa essere memorizzato.
>
> **Nota**
> Le opzioni di scansione per i profili predefiniti possono essere impostate in Configurazione > System Scanner > Scansione > File. È possibile adeguare queste impostazioni alle proprie esigenze.

Drive locali

Viene eseguita una ricerca di virus o programmi indesiderati in tutti i drive locali del sistema.

Hard Disk locali

Viene eseguita una ricerca di virus o programmi indesiderati in tutti gli hard disk locali del sistema.

Drive rimovibili

Viene eseguita una ricerca di virus o programmi indesiderati in tutti i drive rimovibili del sistema.

Directory di sistema di Windows

Viene eseguita una ricerca di virus o programmi indesiderati nella directory di sistema di Windows.

Scansione completa del sistema

Viene eseguita una ricerca di virus o programmi indesiderati in tutti gli hard disk locali del computer. Durante la ricerca vengono eseguite tutte le procedure di scansione e di verifica, ad eccezione del controllo dell'integrità dei file di sistema: scansione standard di file, verifica del registro e dei settori di avvio, ricerca di rootkit, ecc. (vedere System Scanner > Panoramica). Le procedure di verifica vengono eseguite indipendentemente dalle impostazioni di Scanner nella configurazione in System Scanner > Scansione: Impostazioni aggiuntive.

Scansione rapida del sistema

Le cartelle più importanti nel computer (le directory *Windows*, *Programmi*, *Documents and settings\Default User*, *Documents and settings\All Users*) vengono scansionate alla ricerca di virus e programmi indesiderati.

Documenti

Viene eseguita una ricerca di virus o programmi indesiderati nella cartella di default *Documenti* dell'utente registrato.

> **Nota**
> "*Documenti*" in Windows è una directory nel profilo dell'utente utilizzata come cartella di default per i documenti che vengono salvati. Nell'impostazione di default questa directory si trova in *C:\Documents and Settings\[Nome utente]\Documenti*.

Processi attivi

Viene eseguita una ricerca di virus o programmi indesiderati in tutti i processi attivi del sistema.

Scansione alla ricerca di rootkit e malware attivi

Viene eseguita una scansione di rootkit e di malware attivi (aperti) sul computer. Contemporaneamente vengono controllati tutti i processi attivi.

> **Nota**
> Nella modalità interattiva sono disponibili diverse possibilità per procedere dopo il rilevamento. Nella modalità automatica il rilevamento viene segnalato nel file di report.

> **Nota**
> La scansione del rootkit non è disponibile in Windows XP a 64 bit .

7.3.4 Selezione manuale

Se si desidera adattare la ricerca alle proprie esigenze, selezionare questa cartella. Evidenziare le directory e i file che si desidera scansionare.

> **Nota**
> Il profilo **Selezione manuale** serve per scansionare i dati senza creare un nuovo profilo.

Profili personalizzati

È possibile creare un nuovo profilo mediante la barra degli strumenti, mediante collegamento o tramite il menu contestuale.

I nuovi profili possono essere memorizzati con il nome definito dall'utente e sono inoltre utili per la scansione gestita manualmente per la creazione di scansioni pianificate tramite il Pianificatore.

Barra degli strumenti e collegamenti

Icona	Collegamento	Descrizione
	F3	**Avvia la scansione con il profilo selezionato** Viene eseguita una ricerca di virus e programmi indesiderati nel profilo selezionato.
	F6	**Avvia la scansione con il profilo selezionato come amministratore** Il profilo selezionavo viene analizzato con diritti di amministratore.
	Agg	**Crea un nuovo profilo** Viene creato un nuovo profilo.
	F2	**Rinomina il profilo selezionato** Assegna al profilo selezionato il nome scelto dall'utente.
	F4	**Crea un collegamento sul desktop per il profilo selezionato** Crea un collegamento al profilo selezionato sul desktop.
	Canc	**Elimina il profilo selezionato** Il profilo selezionato viene eliminato definitivamente.

Menu contestuale

Per aprire il menu contestuale per questa rubrica, selezionare con il mouse un profilo desiderato quindi fare clic con il pulsante destro del mouse.

Avvia la scansione

Viene eseguita una ricerca di virus e programmi indesiderati nel profilo selezionato.

Avvia la scansione (amministratore)

(Questa funzione è disponibile solo in Windows Vista e sistemi operativi successivi. Per eseguire l'azione è necessario possedere i diritti di amministratore.)

Viene eseguita una ricerca di virus e programmi indesiderati nel profilo selezionato.

Crea un nuovo profilo

Viene creato un nuovo profilo. Selezionare le directory e i file da scansionare.

Rinomina profilo

Assegna al profilo selezionato il nome scelto dall'utente.

> **Nota**
> Questa voce nel menu contestuale non è selezionabile se è stato selezionato un profilo predefinito.

Elimina profilo

Il profilo selezionato viene eliminato definitivamente.

> **Nota**
> Questa voce nel menu contestuale non è selezionabile se è stato selezionato un profilo predefinito.

Filtro file

Standard

Significa che i file vengono sottoposti a scansione in base all'impostazione nel gruppo File della configurazione. Questa impostazione può essere adattata alle proprie esigenze nella configurazione. È possibile accedere alla configurazione mediante il pulsante o il link Configurazione.

Scansiona tutti i file:

Tutti i file vengono scansionati indipendentemente dall'impostazione in Configurazione.

Personalizzato

Viene richiamata una finestra di dialogo in cui vengono visualizzate tutte le estensioni dei file scansionati. Le estensioni includono voci di default. Tuttavia, è possibile aggiungere o eliminare delle voci.

> **Nota**
> È possibile selezionare questa voce nel menu contestuale solo se si posiziona il

mouse su una checkbox.
La selezione dell'opzione non è consentita con i profili predefiniti.

Selezionare

Con sottodirectory:

Nel punto selezionato viene scansionato tutto (segno di spunta nero).

Senza sottodirectory:

Nel punto selezionato vengono scansionati solo i file (segno di spunta verde).

Solo sottodirectory:

Nel punto selezionato vengono scansionate solo le sottodirectory, non i file che si trovano nel punto (segno di spunta grigio, le sottodirectory hanno un segno di spunta nero).

Nessuna selezione:

La selezione viene annullata, il punto attualmente selezionato non viene scansionato (nessun segno di spunta).

Nota
È possibile selezionare questa voce nel menu contestuale solo se si posiziona il mouse su una checkbox.
La selezione dell'opzione non è consentita con i profili predefiniti.

Crea collegamento sul desktop

Crea un collegamento al profilo selezionato sul desktop.

Nota
Questa voce non è selezionabile nel menu contestuale se è stato scelto il profilo Selezione manuale, poiché le impostazioni della Selezione manuale non vengono memorizzate a lungo termine.

7.3.5 Real-Time Protection

La rubrica **Real-Time Protection** mostra le informazioni sui file scansionati e altri dati statistici, che possono essere ripristinati in ogni momento e permette di richiamare il file di report. Informazioni dettagliate sull'ultimo virus o programma indesiderato trovato sono reperibili premendo un pulsante.

Nota
Se il servizio Real-Time Protection non è stato avviato, il pulsante viene

rappresentato in giallo accanto al modulo. Tuttavia, esiste la possibilità di visualizzare il File di report di Real-Time Protection.

Barra degli strumenti

Icona	Descrizione
	Visualizza il file di report Viene visualizzato il file di report di Real-Time Protection.
	Resetta le statistiche Le informazioni statistiche della rubrica vengono azzerate.

Informazioni visualizzate

Ultimo file individuato

Mostra il nome e il percorso dell'ultimo file trovato da Real-Time Protection.

Ultimo malware rilevato

Riporta il nome dell'ultimo virus o programma indesiderato rilevato.

Icona	Descrizione
Informazioni Virus	Facendo clic sull'icona o sul link vengono visualizzate informazioni dettagliate sul virus o sul programma indesiderato, a condizione che si disponga di una connessione attiva a Internet.

Ultimo file scansionato

Mostra il nome e il percorso del file scansionato da Real-Time Protection.

Statistiche

Numero dei file

Mostra il numero dei file finora scansionati.

Numero dei malware rilevati

Mostra il numero di virus o programmi indesiderati finora rilevati.

Numero di file sospetti

Mostra il numero di file segnalati dall'euristica.

Numero dei file eliminati

Mostra il numero dei file finora eliminati.

Numero dei file riparati

Mostra il numero dei file finora riparati.

Numero dei file spostati

Mostra il numero dei file finora spostati.

Numero dei file rinominati

Mostra il numero dei file finora rinominati.

7.3.6 FireWall

Windows Firewall (da Windows 7)

A partire da Windows 7 Avira FireWall non è più contenuto in Avira Ultimate Protection Suite. È tuttavia possibile controllare Windows Firewall tramite il centro di controllo e configurazione.

Nella rubrica FireWall è possibile monitorare lo stato di Windows Firewall e ripristinare le impostazioni consigliate facendo clic sul pulsante **Risoluzione del problema**.

7.3.7 Web Protection

La rubrica **Web Protection** visualizza informazioni sugli URL da verificare, nonché ulteriori dati statistici, che possono essere ripristinati in qualsiasi momento, e permette di richiamare il file di report. Informazioni dettagliate sull'ultimo virus o programma indesiderato trovato sono reperibili premendo un pulsante.

Barra degli strumenti

Icona	Descrizione
	Visualizza il file di report Viene visualizzato il file di report di Web Protection.
	Resetta i dati delle statistiche Le informazioni statistiche della rubrica vengono azzerate.

Informazioni visualizzate

Ultimo URL rilevato

Mostra l'ultimo URL rilevato da Web Protection.

Ultimo virus o programma indesiderato rilevato

Riporta il nome dell'ultimo virus o programma indesiderato rilevato.

Icona/Link	Descrizione
Informazioni Virus	Facendo clic sull'icona o sul link vengono visualizzate informazioni dettagliate sul virus o sul programma indesiderato, a condizione che si disponga di una connessione attiva a Internet.

Ultimo URL scansionato

Mostra il nome e il percorso dell'ultimo URL scansionato da Web Protection.

Statistiche

Numero di URL scansionati

Mostra il numero degli URL finora scansionati.

Numero di messaggi

Mostra il numero di virus o programmi indesiderati finora rilevati.

Numero di URL bloccati

Mostra il numero degli URL finora bloccati.

Numero di URL ignorati

Mostra il numero degli URL finora ignorati.

7.3.8 Mail Protection

La rubrica **Mail Protection** mostra le e-mail verificate, le loro proprietà e altri dati statistici.

> **Nota**
> Se il servizio Mail Protection non è stato avviato, il pulsante viene rappresentato in giallo accanto al modulo. Tuttavia, esiste la possibilità di visualizzare il File di report di Mail Protection. Se questo servizio non è disponibile per il prodotto Avira in uso, il pulsante è disattivato.

> **Nota**
> L'esclusione dei singoli indirizzi e-mail dalla verifica del malware si riferisce solo alle e-mail in ingresso. Per disattivare la verifica delle e-mail in uscita, disattivare nella configurazione l'opzione di verifica delle e-mail in uscita in Mail Protection > Scansione.

Barra degli strumenti

Icona	Descrizione
	Visualizza il file di report Viene visualizzato il file di report di Mail Protection.
	Mostra le proprietà dell'e-mail selezionata Apre una finestra di dialogo con informazioni dettagliate sull'e-mail selezionata.
	Non controllare più la presenza di malware su questo indirizzo e-mail L'indirizzo e-mail selezionato non verrà più sottoposto a controlli per verificare la presenza di virus e programmi indesiderati. È possibile annullare questa impostazione nella configurazione in **Mail Protection > Generale > Eccezioni** (vedere Eccezioni).
	Elimina le e-mail selezionate L'e-mail selezionata verrà eliminata dalla memoria temporanea. Il file tuttavia rimarrà nel programma e-mail.

	Resetta le statistiche Le informazioni statistiche della rubrica vengono azzerate.

E-mail scansionate

In questa sezione vengono visualizzate le e-mail controllate da Mail Protection.

Icona	Descrizione
✅	Non è stato trovato alcun virus o programma indesiderato.
⚠	È stato trovato un virus o un programma indesiderato.

Tipo

Mostra il protocollo utilizzato per la ricezione o l'invio di e-mail:

- POP3: e-mail ricevuta mediante POP3
- IMAP: e-mail ricevuta mediante IMAP
- SMTP: e-mail inviata mediante SMTP

Mittente/Destinatario

Mostra l'indirizzo del mittente dell'e-mail.

Oggetto

Mostra l'oggetto dell'e-mail ricevuta.

Data/Ora

Mostra quando l'e-mail è stata soggetta a controlli per lo spam.

> **Nota**
> Per maggiori informazioni su un'e-mail fare doppio clic sull'e-mail desiderata.

Statistiche

Azione e-mail

Mostra l'azione che viene eseguita quando Mail Protection trova un virus o un programma indesiderato in un'e-mail. Nella modalità interattiva non è disponibile alcuna visualizzazione, poiché l'utente può decidere quale procedimento eseguire in caso di rilevamento.

> **Nota**
> Questa impostazione può essere adattata alle proprie esigenze nella configurazione. Alla configurazione si accede mediante il pulsante o il link Configurazione.

Allegati infetti

Mostra l'azione che viene eseguita quando Mail Protection trova un virus o un programma indesiderato in un allegato infetto. Nella modalità interattiva non è disponibile alcuna visualizzazione, poiché l'utente può decidere quale procedimento eseguire in caso di rilevamento.

> **Nota**
> Questa impostazione può essere adattata alle proprie esigenze nella configurazione. Alla configurazione si accede mediante il pulsante o il link Configurazione.

Numero di e-mail

Mostra il numero delle e-mail scansionate da Mail Protection.

Ultimo messaggio

Riporta il nome dell'ultimo virus o programma indesiderato rilevato.

Numero di messaggi

Mostra il numero dei virus e dei programmi indesiderati rilevati e segnalati finora.

E-mail sospette

Mostra il numero di e-mail segnalate dall'euristica.

Numero di e-mail ricevute

Mostra il numero delle e-mail pervenute.

Numero di e-mail inviate

Mostra il numero delle e-mail spedite.

7.3.9 Safe Browsing

La pagina Safe Browsing mostra quali URL sono stati bloccati a causa di categorie di contenuti vietate, orari di utilizzo di Internet vietati o siti Web bloccati.

Barra degli strumenti

È possibile esportare o eliminare gli eventi selezionati. Per evidenziare più eventi, tenere premuto il tasto **Ctrl** o il tasto **Maiusc** (selezione di eventi consecutivi) durante la selezione degli eventi. Per selezionare tutti gli eventi visualizzati, premere **Ctrl + A**.

Icona	Descrizione
	Mostra l'evento selezionato Apre una finestra in cui vengono visualizzate le proprietà di un evento selezionato. Esempio: *Safe Browsing ha bloccato il sito Web ...* *Il sito Web è stato bloccato per il seguente motivo: Armi / Militarismo.* *Il sito Web è stato richiamato dall'utente...*
	Esporta l'evento(i) selezionato(i) Esporta gli eventi selezionati.
	Elimina l'evento(i) selezionato(i) Elimina gli eventi selezionati.

Informazioni visualizzate

La visualizzazione eventi di Safe Browsing contiene le seguenti informazioni.

- **URL**

  Il sito bloccato da Safe Browsing**.**
- **Categoria**

  Classificazione degli URL bloccati: *Armi / Militarismo, Erotismo / Sesso, Sette, ecc.*.
- **Utente**

  Utente che ha richiamato l'URL bloccato.
- **Data/Ora**

  Data e ora locale in cui si è verificato l'evento.

È possibile ordinare gli eventi facendo clic sul titolo della colonna. In genere gli eventi vengono disposti in ordine cronologico (per **data/ora** in ordine decrescente).

Argomenti correlati:

- Che cos'è Safe Browsing

- Safe Browsing Configurazione

7.3.10 Avira Free Android Security

Avira Free Android Security è un'app che protegge i dispositivi da furto e/o smarrimento. L'app comprende funzioni che consentono di individuare il dispositivo portatile quando è stato messo chissà dove oppure, peggio ancora, in caso di furto. Quest'applicazione permette inoltre di bloccare le telefonate o gli SMS in arrivo. Avira Free Android Security protegge i telefoni cellulari e gli smartphone basati sul sistema operativo Android.

Avira Free Android Security consta di due componenti:

- L'app vera e propria che viene installata sul dispositivo Android
- La console Web Avira Android per la registrazione e il controllo delle funzioni

Avira Free Android Security è un'app gratuita che non richiede alcuna licenza. Avira Free Android Security supporta tutte le marche principali, ad esempio Samsung, HTC, LG e Motorola.

Per ulteriori informazioni consultare il nostro sito Web:

www.avira.com/android

7.3.11 Quarantena

Il **Gestore della quarantena** gestisce gli oggetti infetti (file ed email). Il prodotto Avira può spostare gli oggetti infetti in un formato speciale nella directory della quarantena. Essi non possono quindi essere aperti o eseguiti.

> **Nota**
> Per spostare gli oggetti nel Gestore della quarantena, selezionare l'opzione corrispondente per la quarantena in **Configurazione** sotto **System Scanner** , **Real-Time Protection** e **Mail Protection** dal menu **Scansione > Azione su rilevamento** , se si lavora in **modalità automatica**.
> In alternativa è possibile selezionare nella **modalità interattiva** l'opzione corrispondente per la quarantena.

Barra degli strumenti, shortcut e menu contestuale

Icona	Collegamento	Descrizione
	F2	**Scansiona nuovamente l'oggetto/gli oggetti** Un oggetto selezionato viene nuovamente sottoposto a scansione per individuare virus e programmi indesiderati. In questa procedura vengono utilizzate le impostazioni della scansione diretta.
	Invio	**Proprietà** Apre una finestra di dialogo con informazioni dettagliate sull'oggetto selezionato. **Nota** Le informazioni dettagliate possono essere aperte anche facendo doppio clic su un oggetto.

(Windows Vista)	**F3**	**Ripristina l'oggetto/gli oggetti** Viene ripristinato un oggetto selezionato. Tale oggetto verrà riportato quindi nella posizione originale. **Nota** Questa opzione non è disponibile per gli oggetti del tipo email. **Avviso** Virus e programmi indesiderati causano enormi danni al sistema! Quando si ripristinano i file, assicurarsi che vengano ripristinati solo quei file che possono essere ripuliti con una nuova scansione. **Nota** In Windows Vista e versioni successive, è necessario disporre dei diritti di amministratore per ripristinare gli oggetti.
	F6	**Ripristina l'oggetto/gli oggetti in...** Un oggetto selezionato può essere riportato nella posizione desiderata. Selezionando questa opzione si apre una finestra di dialogo "Salva con nome" in cui è possibile specificare la posizione desiderata. **Avviso** Virus e programmi indesiderati causano enormi danni al sistema! Quando si ripristinano i file, assicurarsi che vengano ripristinati solo quei file che possono essere ripuliti con una nuova scansione.

+	**Agg**	**Aggiungi il file sospetto alla quarantena** Se si ritiene sospetto un file, con questa opzione è possibile aggiungerlo manualmente al Gestore della quarantena. Se opportuno, caricare il file da verificare sul server Web di Avira Malware Research Center tramite l'opzione Invia oggetto/gli oggetti.
	F4	**Invia l'oggetto/gli oggetti** L'oggetto da verificare viene caricato sul server Web di Avira Malware Research Center. Premendo il pulsante **Invia l'oggetto/gli oggetti**, si aprirà dapprima una finestra di dialogo con un modulo per l'inserimento dei dati personali. Indicare per intero i propri dati. Scegliere un tipo: **File sospetto** o **Falso positivo**. Premere **OK** per caricare il file sospetto. **Nota** La dimensione massima dei file caricati è di 20 MB non compressi o 8 MB compressi. **Nota** È possibile caricare solo un singolo file per volta.
×	**Canc**	**Elimina l'oggetto/gli oggetti** Dal Gestore della quarantena viene eliminato un file selezionato. Il file non può essere ripristinato.
		Copia l'oggetto/gli oggetti in... L'oggetto in quarantena selezionato viene archiviato nella directory scelta. **Nota** L'oggetto in quarantena non corrisponde esattamente al file ripristinato. L'oggetto in quarantena è crittografato e non può essere eseguito o letto nel formato originale.

	F7	**Esporta tutte le proprietà** Le proprietà dell'oggetto in quarantena selezionato vengono esportate in un file di testo.
	F10	**Apri directory di quarantena** Apre la cartella INFECTED.

Nota
È possibile eseguire azioni su diversi oggetti selezionati.
Per evidenziare più oggetti, tenere premuto il tasto Ctrl o il tasto Maiusc (selezione di oggetti consecutivi) durante la selezione degli oggetti nel Gestore della quarantena. Per selezionare tutti gli oggetti visualizzati, premere **Ctrl + A.**
Durante l'azione **Mostra proprietà** non è possibile selezionare più oggetti. La selezione multipla non è consentita durante l'esecuzione dell'azione **Invia l'oggetto/gli oggetti** poiché è possibile caricare un file alla volta.

Tabella

Stato

Un oggetto in quarantena può avere stati diversi:

Icona	Descrizione
	Non è stato trovato alcun virus o programma indesiderato, l'oggetto è pulito.
	È stato trovato un virus o un programma indesiderato.
	Se un file sospetto viene aggiunto al Gestore della quarantena mediante l'opzione Aggiungi file, l'utente visualizza un'icona di avvertenza.

Tipo

Definizione	Descrizione
Email	L'oggetto rilevato è un'email.
File	L'oggetto rilevato è un file.

Rilevamento

Mostra il nome del malware rilevato.
I rilevamenti euristici sono identificati dalla sigla HEUR/.

Fonte

Mostra il percorso nel quale è stato trovato l'oggetto.

Data/Ora

Mostra la data e l'ora del rilevamento.

Informazioni dettagliate

Nome del file

Percorso completo e nome file dell'oggetto

Oggetto in quarantena

Nome file dell'oggetto in quarantena

Ripristinato

SÌ/NO

SÌ: l'oggetto è stato ripristinato.

NO: l'oggetto non è stato ripristinato.

Caricato in Avira

SÌ/NO

SÌ: l'oggetto è già stato caricato sul server Web di Avira Malware Research Center

per eseguire le verifiche necessarie.

NO: l'oggetto non è ancora stato caricato sul server Web di Avira Malware Research Center

per eseguire le verifiche necessarie.

Sistema operativo

Workstation Windows XP: il malware è stato rilevato da un prodotto desktop di Avira.

Motore di scansione

Numero di versione del motore di scansione

File di definizione dei virus

Numero di versione del file di definizione dei virus

Rilevamento

Nome del malware rilevato

Data/Ora

Data e ora del rilevamento

7.3.12 Pianificatore

Il **Pianificatore** offre la possibilità di creare job temporalmente pianificato di scansione e aggiornamento nonché di adattare o eliminare job esistenti.

Dopo l'installazione, nell'impostazione standard viene applicato il job seguente:

- Job scansione **Scansione rapida del sistema** (impostazione standard): ogni settimana viene eseguita automaticamente una scansione rapida del sistema. Durante la scansione rapida del sistema viene eseguita una ricerca di virus o programmi indesiderati nei file e nelle cartelle più importanti del computer. Il job di scansione può essere modificato, ma si consiglia di creare altri job di scansione che rispondano meglio alle proprie esigenze.

Barra degli strumenti, shortcut e menu contestuale

Icona	Shortcut	Menu contestuale
+	Agg	**Inserisci nuovo job** Crea un nuovo job. Un assistente guida l'utente tra le impostazioni necessarie.
i	Invio	**Proprietà** Apre una finestra di dialogo con informazioni dettagliate sul job selezionato.
	F2	**Modifica del job** Avvia l'assistente per la creazione e la modifica del job.
×	Canc	**Eliminazione del job** Elimina dall'elenco i job selezionati.

		Visualizza il file di report Viene visualizzato il file di report del Pianificatore.
	F3	Avvio del job Avvia un job selezionato dall'elenco.
	F4	Interruzione del job Arresta un job avviato e selezionato.

Tabella

Tipo di job

Icona	Descrizione
	Il job è un job di aggiornamento.
	Il job è un job di scansione.

Nome

Denominazione job.

Azione

Indica se si tratta di un job di **scansione** o di un **aggiornamento**.

Frequenza

Mostra quando e con che frequenza viene avviato il job.

Modalità di visualizzazione

Sono disponibili le seguenti modalità di visualizzazione:

Invisibile: il job viene eseguito in background e non è visibile. È valido per i job di scansione e di aggiornamento.

Ridotta: la finestra del job mostra solo una barra di avanzamento.

Espansa: la finestra del job è completamente visibile.

Attivato

Il job viene attivato se si attiva una casella di controllo.

> **Nota**
> Se la frequenza del job è stata impostata su Immediata, il job viene avviato subito dopo l'attivazione. In questo modo si ha la possibilità di riavviare il job in caso di necessità.

Stato

Mostra lo stato del job:

Pronto: il job è pronto per essere eseguito.

In esecuzione: il job è stato avviato e si trova in fase di esecuzione.

Creazione di job con il Pianificatore

L'assistente di pianificazione aiuta l'utente nella pianificazione, configurazione e creazione

- di una ricerca temporalmente pianificata di virus e programmi indesiderati
- di un aggiornamento temporalmente pianificato mediante Internet

Per entrambi i tipi di job è necessario indicare

- il nome e la descrizione del job
- quando si deve avviare il job
- con quale frequenza bisogna eseguire il job
- la modalità di visualizzazione del job

Frequenza del job

Opzione	Descrizione
Immediatamente	Il job viene avviato subito al termine dell'assistente di pianificazione.
Ogni giorno	Il job viene avviato giornalmente a un determinato orario, ad esempio alle 22:00.
Ogni settimana	Il job viene avviato settimanalmente in uno o più giorni e a un'ora determinati, ad esempio martedì e venerdì alle 16:26.
Intervallo	Il job viene eseguito in un determinato intervallo, ad esempio ogni 24 ore.

Singolo	Il job viene eseguito solo una volta a un orario definito, ad esempio il 10/04/2004 alle 10:04.
Login	Il job viene eseguito a ogni login di un utente di Windows.

Orario dell'avvio del job

È ora possibile stabilire un giorno della settimana, una data, un'ora o un intervallo in cui avviare il job. Questo non viene visualizzato se è stato selezionato *Immediatamente* come orario dell'avvio.

In base al tipo di job sono presenti diverse opzioni supplementari:

Avvia il job all'avvio della connessione Internet (dial-up)

Oltre alla frequenza stabilita il job viene eseguito quando si attiva una connessione a Internet.
Questa opzione è selezionabile in caso di job di aggiornamento che devono essere eseguiti ogni giorno, ogni settimana o a un intervallo.

Ripeti job se il tempo è scaduto

Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.
Questa opzione è selezionabile sia in caso di job di aggiornamento sia in caso di job di scansione che deve essere eseguito ogni giorno, ogni settimana, a intervalli predefiniti o un'unica volta.

Spegni computer al termine del job

Il computer viene spento dopo che il job è stato eseguito e completato. L'opzione è disponibile per i job di scansione nella modalità di visualizzazione ridotta e estesa.

Nota
Durante un job di scansione nella finestra di dialogo Selezione del profilo è possibile selezionare sia Profili standard predefiniti sia Profili personalizzati. Il profilo Selezione manuale viene eseguito sempre con la selezione attuale.

7.3.13 Report

La rubrica **Report** consente di richiamare i risultati delle azioni eseguite dal programma.

Barra degli strumenti, shortcut e menu contestuale

Icona	Shortcut	Descrizione
	Invio	**Mostra il report** Apre una finestra in cui si visualizza il risultato dell'azione selezionata. Ad esempio il risultato di una scansione.
	F3	**Visualizza il file di report** Mostra il file di report relativo al report selezionato.
	F4	**Stampa il file di report** Apre la finestra di dialogo Stampa di Windows per la stampa del file di report.
	Canc	**Elimina il report** Elimina il report selezionato e il relativo file di report.

Tabella

Stato

Icona	Descrizione
	Azione scansione: nessun rilevamento
	Azione scansione: rilevamento di virus o non conclusa con successo
	Azione aggiornamento: aggiornamento concluso correttamente
	Azione aggiornamento: aggiornamento non riuscito

Azione

Mostra l'azione intrapresa.

Risultato

Mostra il risultato dell'azione.

Data/Ora

Mostra la data e l'ora di creazione del report.

Contenuto di un report per una scansione

- *Data della scansione:*

  Data della scansione.
- *Ora di inizio della scansione:*

  Ora di inizio della scansione.
- *Tempo richiesto per la scansione:*

  Mostra il tempo nel formato mm:ss.
- *Stato della scansione:*

  Mostra se il job di scansione è stato eseguito completamente o è stato interrotto.
- *Ultimo rilevamento:*

  Nome dell'ultimo virus o programma indesiderato rilevato.
- *Directory scansionate:*

  Numero complessivo delle directory scansionate.
- *File scansionati:*

  Numero complessivo dei file scansionati.
- *Archivi scansionati:*

  Numero degli archivi scansionati.
- *Oggetti nascosti:*

  Numero complessivo degli oggetti nascosti trovati.
- *Rilevamenti:*

  Numero complessivo di virus o programmi indesiderati rilevati.
- *Sospetti:*

  Numero di file sospetti.
- *Avvisi:*

  Numero degli avvisi di rilevamento di virus.
- *Note:*

Numero delle note create, ad esempio ulteriori informazioni che possono emergere durante una scansione.

- *Riparati:*

  Numero complessivo dei file riparati.

- *Quarantena:*

  Numero complessivo dei file spostati in quarantena.

- *Rinominati:*

  Numero complessivo dei file rinominati

- *Eliminati:*

  Numero complessivo dei file eliminati.

- *Sovrascritti:*

  Numero complessivo dei file sovrascritti.

> **Nota**
> I rootkit hanno la capacità di nascondere processi e oggetti, ad esempio voci di registro o file, ma non tutti gli oggetti nascosti sono necessariamente indicatori dell'esistenza di un rootkit. Gli oggetti nascosti possono anche essere oggetti innocui. Se durante la scansione vengono trovati oggetti nascosti ma non viene visualizzato nessun messaggio d'avviso indicante il rilevamento di virus, in base al report occorre stabilire di quali oggetti si tratta e recuperare maggiori informazioni sugli oggetti trovati.

7.3.14 Eventi

In **Eventi** vengono visualizzati gli eventi creati di diversi componenti del programma.

Gli eventi sono memorizzati in una banca dati. È possibile limitare l'estensione della banca dati degli eventi o disattivare la limitazione dell'estensione della banca dati (vedere Eventi). Nell'impostazione standard vengono memorizzati solo gli eventi degli ultimi 30 giorni. La visualizzazione degli eventi viene aggiornata automaticamente selezionando la rubrica **Eventi**.

> **Nota**
> L'aggiornamento automatico della visualizzazione con la selezione della rubrica non avviene se nella banca dati eventi sono memorizzati più di 20.000 eventi. In questo caso, premere F5 per aggiornare la visualizzazione eventi.

Barra degli strumenti, shortcut e menu contestuale

Icona	Shortcut	Descrizione
	Invio	**Mostra l'evento selezionato** Si apre una finestra in cui viene visualizzato il risultato di un'azione selezionata. Ad esempio, il risultato di una scansione.
	F3	**Esporta l'evento(i) selezionato(i)** Esporta gli eventi selezionati.
	Canc	**Elimina l'evento(i) selezionato(i)** Elimina l'evento selezionato.

Nota
È possibile eseguire azioni su diversi eventi selezionati. Per evidenziare più eventi, tenere premuto il tasto Ctrl o il tasto Maiusc (selezione di eventi consecutivi) durante la selezione degli eventi. Per selezionare tutti gli eventi visualizzati, premere Ctrl + A.
Durante l'azione Mostra l'evento selezionato non è possibile eseguire la selezione di numerosi oggetti.

Moduli

Gli eventi dei seguenti moduli (qui in ordine alfabetico) possono essere presentati con l'aiuto della visualizzazione eventi:

Definizione del modulo
Web Protection
Real-Time Protection
Mail Protection
Servizio di assistenza

Pianificatore
Safe Browsing
Scanner
Updater

Con un segno di spunta nella casella **Tutti** è possibile visualizzare gli eventi di tutti i moduli disponibili. Per visualizzare solamente gli eventi di un modulo specifico, selezionare la casella di controllo accanto al modulo desiderato.

Filtro

Nella visualizzazione eventi vengono visualizzati questi tipi di eventi:

Icona	Descrizione
	Informazione
	Avviso
	Errore
	Rilevamento

Con un segno di spunta nella casella di controllo **Filtro** è possibile visualizzare tutti gli eventi. Per visualizzare solamente determinati eventi, selezionare la casella di controllo accanto all'evento desiderato.

Tabella

La visualizzazione eventi contiene le seguenti informazioni:

Icona

L'icona per la rappresentazione del tipo di file.

Tipo

Classificazione dell'evento: informazione, avviso, errore, rilevamento.

Modulo

Il modulo Avira in cui si è verificato l'evento. Ad esempio Real-Time Protection che ha effettuato un rilevamento.

Azione

Descrizione dell'evento del modulo.

Data/Ora

Data e ora locale in cui si è verificato l'evento.

7.3.15 Aggiorna

Aggiorna la visualizzazione della rubrica aperta.

7.4 Extra

7.4.1 Scansione dei record di avvio

È possibile analizzare con la scansione diretta anche i settori di avvio dei drive della workstation. Quest'operazione è consigliabile se durante la scansione diretta è stato trovato un virus e si desidera controllare che i settori di avvio non siano infetti.

Per selezionare più settori di avvio, selezionare con il mouse i drive desiderati tenendo premuto il tasto Maiusc.

> **Nota**
> È possibile far analizzare automaticamente i settori di avvio a ogni scansione diretta (v. Scansiona settori di avvio dei drive).

> **Nota**
> A partire da Windows Vista, la scansione dei settori di avvio è possibile solo se si è in possesso dei diritti di amministratore.

7.4.2 Elenco dei rilevamenti

Con questa funzione vengono elencati i nomi di virus e programmi indesiderati riconosciuti dal prodotto Avira. È integrata una semplice funzione di scansione per i nomi.

Ricerca nell'elenco dei rilevamenti

Nel campo *Cerca:* inserire una stringa di ricerca o una sequenza di caratteri.

Cerca sequenza di caratteri all'interno di un nome

È possibile inserire sulla tastiera una sequenza di lettere o caratteri, l'evidenziazione passa al primo posto dell'elenco dei nomi in cui si rileva tale sequenza di caratteri - anche al centro di un nome - (esempio: inserendo "raxa" si troverà "Abraxas").

Cerca dal primo carattere di un nome

È possibile inserire qui le lettere iniziali e i caratteri successivi sulla tastiera, l'evidenziazione sfoglia alfabeticamente l'elenco dei nomi (esempio: inserendo "co" si troverà "coniglio").

Se il nome o la sequenza di caratteri ricercati sono disponibili, la corrispondenza viene evidenziata nell'elenco.

Cerca avanti

Avvia la ricerca in avanti in ordine alfabetico.

Cerca indietro

Avvia la ricerca all'indietro in ordine alfabetico.

Prima corrispondenza

Torna alla prima voce rilevata nell'elenco.

Voci nell'elenco dei rilevamenti

Sotto questo titolo si trova un elenco di nomi di virus e programmi indesiderati che possono essere riconosciuti. La maggior parte delle voci di questo elenco possono essere eliminate anche con il prodotto Avira. Sono elencati in ordine alfabetico (prima caratteri speciali e numeri, poi lettere). Utilizzare la barra di scorrimento per spostarsi verso il basso o di nuovo verso l'alto nell'elenco.

7.4.3 Scaricare il CD di ripristino

Il comando **Scaricare il CD di ripristino** consente di scaricare il pacchetto del CD di ripristino Avira. Il pacchetto contiene un sistema live avviabile per PC nonché uno scanner antivirus Avira con il file di definizione dei virus e il motore di ricerca più aggiornati. In caso di danni al sistema operativo, utilizzare il CD di emergenza Avira per riavviare il PC dal CD o dal DVD, per salvare i dati o per eseguire una scansione alla ricerca di virus e malware.

Al termine del download del pacchetto del CD di ripristino Avira viene visualizzata una finestra di dialogo in cui selezionare il drive CD/DVD per masterizzare il CD di ripristino. È inoltre possibile salvare il pacchetto del CD di ripristino Avira per masterizzare il CD di emergenza in un secondo tempo.

Nota
Per scaricare il pacchetto del CD di ripristino Avira è necessario disporre di una

connessione a Internet attiva. Per masterizzare il CD di emergenza sono necessari un'unità CD-/DVD e un CD/DVD riscrivibile.

7.4.4 Configurazione

La voce di menu **Configurazione** del menu **Extra** permette di aprire la Configurazione.

7.5 Aggiornamento

7.5.1 Avvia l'aggiornamento...

La voce di menu **Avvia l'aggiornamento...** nel menu **Aggiornamento** avvia un aggiornamento immediato. Il file di definizione dei virus e il motore di ricerca vengono aggiornati.

7.5.2 Aggiornamento manuale...

La voce **Aggiornamento manuale...** del menu **Aggiornamento** apre una finestra di dialogo per scegliere e caricare un pacchetto di aggiornamenti per definizioni dei virus e motore di ricerca. Il pacchetto di aggiornamento può essere scaricato dal sito Web del produttore e contiene il file di definizione dei virus e il motore di scansione attuali: http://www.avira.com/it

Nota
A partire da Windows Vista, è necessario disporre dei diritti di amministratore per eseguire un aggiornamento manuale.

7.6 Guida

7.6.1 Argomenti

La voce di menu **Argomenti** nel menu **Guida in linea** apre l'indice della guida in linea.

7.6.2 Aiutami

Se la connessione a Internet è attiva, la voce di menu **Aiutami** del menu **Guida in linea** consente di aprire la pagina del supporto rilevante per il prodotto in uso sul sito Web Avira. Da questa pagina è possibile leggere le risposte alle domande frequenti, richiamare il Knowledge Base o contattare il servizio clienti Avira.

7.6.3 Supporto live

Se è presente una connessione a Internet attiva, il comando **Supporto live** nel menu **Guida in linea** apre la pagina Web di Avira. Scaricare il tool Avira Support Customer Module. Il modulo di assistenza è necessario per il collegamento in remoto al servizio di supporto Avira. Al termine del download e dell'installazione del modulo, contattare telefonicamente il team di supporto Avira per comunicare l'ID del modulo e fissare un appuntamento per la manutenzione remota.

7.6.4 Forum

Se è presente una connessione a Internet attiva, la voce di menu **Forum** del menu **Guida** apre una pagina Web da cui si può accedere al forum di Avira.

7.6.5 Download manuale

Se è presente una connessione a Internet attiva, la voce di menu **Download manuale** del menu **Guida in linea** apre la pagina di download del prodotto Avira. In questa pagina è disponibile il collegamento per il download della versione più aggiornata del manuale del prodotto Avira.

7.6.6 Gestione delle licenze

La voce **Gestione delle licenze** del menu **Guida in linea** apre l'assistente per l'installazione della licenza. Tale assistente aiuta l'utente a installare la licenza del prodotto Avira in uso e ad attivare il prodotto in modo semplice e chiaro.

Attivazione del prodotto

Attivare quest'opzione se si è già in possesso di un codice di attivazione e il prodotto Avira non è ancora stato attivato. Durante l'attivazione del prodotto, l'utente viene registrato come cliente, mentre il prodotto Avira viene attivato con la licenza dell'utente. Il codice di attivazione è stato inviato per e-mail oppure è indicato sulla confezione del prodotto.

> **Nota**
> L'attivazione del programma può essere eseguita ripetutamente con un codice di attivazione valido, qualora sia necessario per via di una nuova installazione del sistema.

> **Nota**
> Per attivare il prodotto, il programma comunica con i server Avira tramite il protocollo HTTP e la porta 80 (comunicazione Web) nonché tramite il protocollo di codifica SSL e la porta 443. Se si utilizza un firewall, assicurarsi che la

connessione necessaria e i dati in entrata e in uscita non vengano bloccati dal firewall.

Nota
È possibile avviare un aggiornamento a un prodotto della famiglia Avira Desktop (vedere Licenza e aggiornamento). Immettere nell'apposito campo il codice di attivazione del prodotto di cui si desidera effettuare l'aggiornamento. Se l'aggiornamento è possibile, il prodotto viene installato automaticamente.

Acquista/Estendi licenza

Questa opzione viene visualizzata quando la licenza è scaduta, quando è ancora valida oppure se si dispone solo di una licenza di evaluation. Utilizzare questa opzione per estendere la licenza del prodotto o per acquistare una licenza completa. A tal fine è necessario disporre di una connessione a Internet attiva: selezionare l'opzione *Acquista/Estendi licenza* e fare clic su **Avanti**. Verrà visualizzato il browser Internet e si accederà al negozio online Avira, dove è possibile acquistare la licenza.

File di licenza valido

Tramite il link **File di licenza** è possibile caricare un file di licenza valido.
Il file di licenza viene generato durante la procedura di attivazione del prodotto tramite un codice di attivazione valido e archiviato e caricato nella directory del programma del prodotto Avira in uso. Utilizzare quest'opzione se è già stata eseguita un'attivazione del prodotto.

Impostazioni proxy...

Facendo clic su questo pulsante si apre una finestra di dialogo. Se necessario, qui è possibile indicare che si desidera stabilire la connessione a Internet, necessaria per l'attivazione del prodotto, tramite un server proxy.

7.6.7 Consiglia prodotto

Se è presente una connessione a Internet attiva, il comando **Consiglia prodotto** nel menu **Guida in linea** apre una pagina Web per i clienti Avira. Qui è possibile consigliare ad altri il prodotto Avira in uso e prendere parte così agli sconti di Avira.

7.6.8 Invia feedback

Se è presente una connessione a Internet attiva, il comando **Feedback** nel menu **Guida in linea** apre una pagina di feedback sui prodotti di Avira GmbH. Qui è riportato un modulo

per la valutazione del prodotto che è possibile inviare ad Avira con le proprie opinioni riguardanti la qualità del prodotto e ulteriori suggerimenti.

7.6.9 Informazioni su Avira Ultimate Protection Suite

Generale

Indirizzi e informazioni relative al prodotto Avira

Informazioni sulla versione

Informazioni sulla versione dei dati inclusi nel pacchetto di prodotti Avira

Informazioni sulla licenza

Dati sulla licenza corrente e collegamento al negozio online (acquisto o estensione di una licenza)

Nota
dati della licenza possono essere collocati nella memoria temporanea. Fare clic con il tasto destro del mouse nella sezione Dati della licenza. Apparirà un menu contestuale. Fare clic nel menu contestuale sul comando **Copia in archivio temporaneo**. I dati della licenza sono ora salvati nell'archivio temporaneo e possono essere aggiunti a e-mail, formulari o documenti mediante il comando Aggiungi di Windows.

8. Protezione dei bambini

Utilizzare le funzioni di Avira *PROTEZIONE DEI BAMBINI* per garantire a bambini o ad altri utenti che utilizzano il computer un'esperienza di navigazione su Internet sicura.

- Mediante la funzione **Safe Browsing** è possibile assegnare ruoli utente agli utenti di Windows. È possibile definire per ciascun ruolo quali URL o categorie di contenuti vietare o consentire, nonché stabilire la durata quotidiana di utilizzo di Internet oppure periodi di utilizzo consentiti.

Argomenti correlati:

- Informazioni su Safe Browsing

8.1 Safe Browsing

Il programma Avira in uso è provvisto della funzione **Safe Browsing** per filtrare offerte Internet indesiderate o illegali e per la limitazione temporale dell'utilizzo di Internet. La funzione **Safe Browsing** fa parte del componente *PROTEZIONE DEI BAMBINI*.

È possibile assegnare ruoli utente agli utenti del computer. I ruoli utente sono configurabili e comprendono un set di regole con i seguenti criteri:

- URL consentiti o non consentiti (indirizzi Internet)
- Categorie di contenuti non consentite
- Durata dell'utilizzo di Internet ed eventuali intervalli di tempo consentiti per l'utilizzo nei giorni della settimana

Per bloccare i contenuti Internet in base a determinate categorie vengono utilizzati elenchi di filtri URL efficaci, nei quali gli URL vengono categorizzati in gruppi di contenuti in base ai contenuti delle pagine Internet. Gli elenchi dei filtri URL vengono aggiornati, adattati e ampliati più volte ogni ora. I ruoli **bambino**, **adolescente**, **adulto** sono preconfigurati con le categorie non consentite corrispondenti.

L'utilizzo temporale di Internet viene stabilito sulla base di richieste di collegamento a Internet che avvengono con un intervallo minimo di 5 minuti.

Se la funzione **Safe Browsing** è attivata, durante la navigazione in Internet tutti i siti Web richiesti nel browser vengono verificati in base al ruolo utente. In caso di siti Web non consentiti, il sito Web viene bloccato e viene visualizzato un messaggio nel browser. In caso di superamento della durata di utilizzo consentita oppure se l'utilizzo supera l'intervallo consentito, le pagine Web richiamate vengono bloccate. Nel browser viene visualizzato un messaggio.

> **Avviso**
> Ricordarsi di attivare il servizio "**Web Protection**" per poter utilizzare la funzione "**Safe Browsing**".

> **Avviso**
> Se viene attivata la funzione **Safe Browsing**, proteggere la configurazione del prodotto Avira in uso tramite una password. Se la configurazione non è protetta tramite password, tutti gli utenti del computer potranno modificare o disattivare le impostazioni in **Safe Browsing**. È possibile attivare la password in Configurazione > Generale > Password.

Argomenti correlati:

- Attiva Safe Browsing
- Assegnazione di un ruolo
- Configurazione di Safe Browsing

8.1.1 Attiva Safe Browsing

- Aprire Avira Control Center e fare clic su **Stato** nella barra di navigazione.

  È necessario attivare **Web Protection** per poter utilizzare la funzione **Safe Browsing**.

- Se non è ancora attivo, attivare **Web Protection** facendo clic sul pulsante rosso accanto a **Web Protection** nella visualizzazione *Stato* in **Sicurezza Internet**.

  Se è attivo, il pulsante accanto a **Web Protection** diventa verde ("attivo").

  Attivare la funzione **Safe Browsing** facendo clic nella visualizzazione **Stato** sul pulsante rosso accanto a **Safe Browsing**.

  Se la funzione è attiva, il pulsante accanto a Safe Browsing diventa verde.

- Per configurare il ruolo di un bambino o di un'altra persona in **Safe Browsing**, fare clic nella visualizzazione **Stato** sul pulsante di configurazione accanto a **Safe Browsing**.

Argomenti correlati:

- Informazioni su Safe Browsing
- Assegnazione di un ruolo
- Configurazione di Safe Browsing

8.1.2 Assegnazione di un ruolo

Prerequisiti:

- ✓ Assicurarsi che per ogni persona che può usare il computer sia stato creato un account utente Windows. Nel prodotto Avira in uso è possibile assegnare ad ogni account utente di Windows un ruolo di Safe Browsing.
- ✓ Attivare la funzione **Safe Browsing** nel prodotto Avira in uso.
- ✓ Prima di assegnare il ruolo a un utente, verificare le proprietà di ogni ruolo.

▸ Nella visualizzazione **Stato** fare clic sul pulsante di configurazione accanto a **Safe Browsing**.

▸ Dall'elenco **Selezione utente** selezionare l'utente al quale si desidera assegnare un ruolo.

L'elenco contiene gli account utente di Windows creati sul computer.

▸ Fare clic su **Aggiungi**.

↳ L'utente viene aggiunto all'elenco.

In Avira Internet Security sono preconfigurati i seguenti ruoli utente:

- **Bambino**
- **Adolescente**
- **Adulto**

Se si aggiunge un account utente all'elenco, il ruolo **Bambino** viene assegnato in base alle impostazioni standard.

▸ È possibile assegnare un altro ruolo facendo clic più volte sul ruolo di un utente.

> **Nota**
> Gli utenti del computer a cui non è stato assegnato nessun ruolo nella configurazione della funzione **Safe Browsing** vengono assegnati per impostazioni standard all'utente **Standard** con il ruolo **Bambino**. È possibile modificare il ruolo dell'utente **standard**.

▸ Fare clic su **Rileva** per salvare la configurazione.

Argomenti correlati:

- Modifica delle proprietà di un ruolo
- Aggiunta o eliminazione di un ruolo

8.1.3 Modifica delle proprietà di un ruolo

▸ Nella visualizzazione **Stato** fare clic sul pulsante di configurazione accanto a **Safe Browsing**.

↳ Le opzioni **Ruoli** vengono visualizzate nella finestra di configurazione della funzione **Safe Browsing**.

▸ Fare clic sul nome del ruolo da modificare (ad esempio **Adolescente**), poi fare clic su **Modifica**.

↳ Verrà visualizzata la finestra con le **Proprietà** del ruolo.

- Apportare le modifiche e fare clic su **OK**.

Argomenti correlati:

- Proprietà del ruolo
- Configurazione di Safe Browsing

8.1.4 Aggiunta o eliminazione di un ruolo

- Nella visualizzazione **Stato** fare clic sul pulsante di configurazione accanto a **Safe Browsing**.

  ↳ Le opzioni **Ruoli** vengono visualizzate nella finestra di configurazione della funzione **Safe Browsing**.

- Per eliminare un ruolo (ad esempio **Adolescente**), fare clic su **Elimina**.

Nota
I ruoli non possono essere eliminati finché sono assegnati a un utente.

- Per aggiungere un ruolo, inserire nel campo di immissione un nome per il ruolo della lunghezza massima di 30 caratteri e fare clic su **Aggiungi**.
- Per adeguare le proprietà del nuovo ruolo, selezionare dall'elenco il nuovo ruolo e fare clic su **Modifica**.

Argomenti correlati:

- Configurazione di Safe Browsing
- Proprietà del ruolo
- Assegnazione di un ruolo

9. Protezione mobile

Avira protegge non solo i computer da malware e virus, ma anche i telefoni cellulari e gli smartphone con sistema operativo Android da furto e/o smarrimento. Grazie alla blacklist di Avira Free Android Security, è possibile bloccare le chiamate e gli SMS indesiderati. È sufficiente aggiungere alla blacklist i numeri di telefono da bloccare estrapolandoli dal Registro chiamate, dall'elenco dei messaggi o dall'elenco dei contatti oppure inserendoli manualmente.

Per ulteriori informazioni consultare il nostro sito Web:

www.avira.com/android

10. Configurazione

10.1 Configurazione

- Opzioni di configurazione in sintesi
- Pulsanti

Opzioni di configurazione in sintesi

Sono disponibili le seguenti opzioni di configurazione:

- **System Scanner**: configurazione della scansione diretta
  - Opzioni di ricerca
  - Azione in caso di rilevamento
  - Opzioni per la scansione degli archivi
  - Eccezioni della scansione diretta
  - Euristica della scansione diretta
  - Impostazione della funzione di report
- **Real-Time Protection**: configurazione della scansione in tempo reale
  - Opzioni di ricerca
  - Azione in caso di rilevamento
  - Eccezioni della scansione in tempo reale
  - Euristica della scansione in tempo reale
  - Impostazione della funzione di report
- **Aggiornamento**: configurazione delle impostazioni di aggiornamento
  - Download tramite server Web
- **Web Protection**: configurazione di Web Protection
  - Opzioni di scansione, attivazione e disattivazione di Web Protection
  - Azione in caso di rilevamento
  - Accessi bloccati: tipi di file e tipi di MIME indesiderati, Filtro Web per URL noti indesiderati (malware, phishing, ecc.)
  - Eccezioni di scansioni di Web Protection: URL, tipi di file, tipi di MIME
  - Euristica di Web Protection
  - Impostazione della funzione di report
- **Mail Protection**: configurazione di Mail Protection
  - Opzioni di scansione: attivazione del monitoraggio degli account POP3, account IMAP e delle e-mail in uscita (SMTP)
  - Azione in caso di rilevamento
  - Altre azioni

- Euristica della scansione di Mail Protection
- Funzione AntiBot: server SMTP consentiti, mittenti e-mail consentiti
- Eccezioni della scansione di Mail Protection
- Configurazione della memoria temporanea, svuota la memoria temporanea
- Configurazione di un piè di pagina nelle e-mail inviate
- Impostazione della funzione di report

- **Protezione dei bambini**:
  - Safe Browsing: funzione di protezione dei bambini con filtro basato sui ruoli e limitazione temporale dell'utilizzo di Internet basata sui ruoli
- **Generale**:
  - Categorie estese delle minacce per la scansione diretta e in tempo reale
  - Protezione avanzata: opzioni di attivazione di ProActiv e Protection Cloud
  - Filtro applicazioni: blocco o autorizzazione delle applicazioni
  - Protezione con password per l'accesso al Control Center e alla configurazione
  - Sicurezza: blocco esecuzione automatica, limitazione per file host di Windows, tutela del prodotto
  - WMI: attiva supporto WMI
  - Configurazione del log eventi
  - Configurazione delle funzioni di report
  - Impostazione delle directory utilizzate
  - Configurazione degli avvisi acustici in caso di rilevamento malware

Pulsanti

Pulsanti	Descrizione
Valori standard	Tutte le impostazioni dei valori standard nella configurazione vengono ripristinate. Quando si ripristinano i valori standard tutte le modifiche e le immissioni dell'utente vengono perse.
OK	Tutte le impostazioni definite vengono memorizzate. La configurazione si chiude. La gestione account cliente (UAC) necessita del vostro consenso per applicare i cambiamenti effettuati nel sistema operativo a partire da Windows Vista.

Annulla	La configurazione viene chiusa senza memorizzare le impostazioni definite dall'utente nella configurazione.
Applica	Tutte le impostazioni definite vengono memorizzate. La gestione account cliente (UAC) necessita del vostro consenso per applicare i cambiamenti effettuati nel sistema operativo a partire da Windows Vista.

10.2 Scanner

La rubrica **Scanner** della configurazione è dedicata alla configurazione della scansione diretta, ovvero alla scansione su richiesta.

10.2.1 Scansione

Qui si può definire la procedura standard della routine di scansione durante una scansione diretta. Se si seleziona una determinata directory da controllare durante la scansione diretta, Scanner esegue i controlli in base alla configurazione:

- con una determinata prestazione di scansione (priorità),
- anche sui record di avvio e nella memoria principale,
- su tutti i file o i file selezionati nella directory.

File

Scanner può utilizzare un filtro per scansionare solamente i file con una determinata estensione (tipo).

Tutti i file

Se l'opzione è attivata, viene eseguita una ricerca di virus e programmi indesiderati in tutti i file indipendentemente dal contenuto e dall'estensione. Il filtro non viene utilizzato.

> **Nota**
> Se **Tutti i file** è attivo, il pulsante **Estensioni file** non è selezionabile.

Utilizza estensioni smart

Se l'opzione è attivata, la selezione dei file da scansionare viene effettuata automaticamente dal programma. Ciò significa che il prodotto Avira decide, in base al contenuto di un file, se quest'ultimo deve essere controllato o meno per verificare la presenza di virus e programmi indesiderati. Questa procedura è lievemente più lenta di **Utilizza l'elenco delle estensioni**, ma molto più sicura poiché i controlli non

vengono effettuati solamente sulla base delle estensioni dei file. Questa impostazione è attivata di default ed è consigliata.

> **Nota**
> Se **Utilizza estensioni smart** è attivo, il pulsante **Estensioni file** non è selezionabile.

Utilizza l'elenco delle estensioni

Se l'opzione è attivata, vengono scansionati solo i file con una determinata estensione. Sono preimpostati tutti i tipi di file che possono contenere virus e programmi indesiderati. L'elenco può essere modificato manualmente mediante il pulsante "**Estensioni file"**.

> **Nota**
> Se questa opzione è attiva e tutte le voci dell'elenco delle estensioni dei file sono state eliminate, viene visualizzato il testo "*Nessuna estensione dei file*" sotto il pulsante **Estensioni file**.

Estensioni file

Con questo pulsante viene richiamata una finestra di dialogo nella quale sono riportate tutte le estensioni dei file che vengono controllate durante una scansione in modalità "**Utilizza l'elenco delle estensioni**". Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o rimuovere voci.

> **Nota**
> Prestare attenzione al fatto che l'elenco standard può variare da versione a versione.

Impostazioni aggiuntive

Scansiona settori di avvio dei drive

Se l'opzione è attivata, Scanner controlla i record di avvio dei drive selezionati durante la scansione diretta. Questa impostazione è attivata di default.

Scansione dei record master di avvio

Se l'opzione è attivata, Scanner controlla i record master di avvio degli/dell'hard disk utilizzati/o nel sistema.

Ignora i file offline

Se l'opzione è attivata, la scansione diretta ignora completamente i cosiddetti file offline durante la scansione. Ciò significa che in questi file non viene controllata la presenza di virus e programmi indesiderati. I file offline sono i file che sono stati

archiviati fisicamente dall'hard disk, ad es. su un nastro, mediante il cosiddetto sistema gerarchico di gestione della memoria (HSM). Questa impostazione è attivata di default.

Controllo di integrità dei file di sistema

Se l'opzione è attivata, i principali file di sistema di Windows vengono sottoposti a una verifica particolarmente sicura durante ogni scansione diretta per verificare la presenza di modifiche dovute a malware. Se viene individuato un file modificato, questo viene segnalato come rilevamento sospetto. La funzionalità occupa molta memoria. Per questo motivo l'opzione è disattivata di default.

Nota
L'opzione è disponibile solo a partire da Windows Vista.

Nota
Se si utilizzano strumenti di terze parti, si modificano i file di sistema o si personalizza la schermata di avvio, questa opzione non deve essere utilizzata. Questi strumenti sono, ad esempio, i cosiddetti skinpack, TuneUp Utilities o Vista Customization.

Scansione ottimizzata

Se l'opzione è attivata, durante la scansione di Scanner la capacità del processore viene utilizzata in modo ottimale. Per motivi di performance, in caso di scansione ottimale, la funzione di log si verifica al massimo a un livello standard.

Nota
L'opzione è disponibile solo per computer multiprocessore.

Seguire link simbolici

Se l'opzione è attivata, Scanner esegue una scansione di tutti i collegamenti simbolici nel profilo di ricerca o nelle directory selezionate, allo scopo di scansionare i file collegati alla ricerca di virus e malware.

Nota
L'opzione non comprende i collegamenti (shortcut), bensì si riferisce esclusivamente ai link simbolici (generati con mklink.exe) o ai punti di giunzione (generati con junction.exe), presenti in modalità trasparente nel file system.

Scansione rootkit all'avvio

Se l'opzione è attivata, Scanner verifica all'avvio della scansione la presenza di rootkit attivi nella directory di sistema Windows tramite una cosiddetta procedura rapida. Questa procedura non verifica se nel computer vi sono rootkit attivi così dettagliatamente come il profilo di ricerca "**Cerca Rootkits**", ma è molto più rapida. Questa opzione modifica soltanto le impostazioni dei profili creati dall'utente.

> **Nota**
> La scansione dei rootkit non è disponibile in Windows XP a 64 Bit !

Scansiona registro

Se l'opzione è attivata, viene scansionato il registro alla ricerca di software dannosi. Questa opzione modifica soltanto le impostazioni dei profili creati dall'utente.

Ignorare i file e i percorsi di drive di rete

Se l'opzione è attivata, i drive di rete collegati al computer vengono esclusi dalla scansione diretta. Questa opzione è consigliata se i server o altre workstation sono protette da un software antivirus. Questa opzione è disattivata di default.

Processo di scansione

Permetti l'arresto

Se l'opzione è attivata, la ricerca di virus o programmi indesiderati può essere arrestata in ogni momento con il pulsante "**Arresta**" nella finestra "**Luke Filewalker**". Se questa impostazione è disattivata, il pulsante **Arresta** nella finestra "**Luke Filewalker**" è grigio. Pertanto non è possibile terminare prematuramente una scansione. Questa impostazione è attivata di default.

Priorità del sistema di scansione

Scanner differenzia tre livelli di priorità nella scansione diretta. Si tratta di un sistema efficace solo se sul computer sono in esecuzione più processi contemporaneamente. La scelta si ripercuote anche sulla velocità di scansione.

Livello basso

Scanner riceve dal sistema operativo il tempo del processore solo se nessun altro processo necessita di tempo di elaborazione, ovvero finché il sistema di scansione è l'unico programma in esecuzione, la velocità è massima. Nel complesso, in questo modo viene gestito molto bene anche il lavoro con altri programmi: il computer è più veloce se altri programmi sono in esecuzione, mentre Scanner lavora in background.

Livello medio

Scanner viene eseguito con priorità normale. Tutti i processi ricevono lo stesso tempo di elaborazione dal sistema operativo. Questa impostazione è attivata di default ed è

consigliata. In alcune circostanze il lavoro con altre applicazioni ne risulta compromesso.

Livello elevato

Scanner riceve la massima priorità. Un lavoro parallelo con altre applicazioni è pressoché impossibile. Tuttavia Scanner completa la scansione in maniera estremamente rapida.

Azione in caso di rilevamento

È possibile definire le azioni che Scanner deve eseguire quando viene rilevato un virus o un programma indesiderato.

Interattivo

Se l'opzione è attivata, i rilevamenti della scansione di Scanner vengono notificati in una finestra di dialogo. Al termine della scansione di Scanner, si riceve un avviso con l'elenco dei file infetti rilevati. Mediante il menu contestuale è possibile selezionare un'azione da eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure chiudere Scanner.

> **Nota**
> Di default nella finestra di dialogo è preselezionata l'azione **Quarantena**. È possibile selezionare ulteriori azioni mediante il menu contestuale.

Automatico

Se l'opzione è attivata, in caso di rilevamento di virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. Scanner reagisce conformemente alle impostazioni definite precedentemente dall'utente in questa sezione.

Copia il file in quarantena prima dell'azione

Se l'opzione è attivata, Scanner crea una copia di sicurezza (backup) prima dell'esecuzione delle azioni primarie e secondarie desiderate. La copia di sicurezza viene mantenuta in quarantena dove il file può essere ripristinato se possiede un valore informativo. Inoltre è possibile inviare la copia di sicurezza ad Avira Malware Research Center per ulteriori indagini.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando Scanner rileva un virus o un programma indesiderato. Se l'opzione "**Ripara**" è attiva, ma la riparazione del file infetto non è possibile, verrà eseguita l'azione definita in "**Azione secondaria**".

> **Nota**
> L'opzione **Azione secondaria** è selezionabile solo se in **Azione primaria** è stata selezionata l'impostazione **Ripara**.

Ripara

Se l'opzione è attivata, Scanner ripara automaticamente i file infetti. Se Scanner non può riparare un file infetto, in alternativa esegue l'opzione selezionata in Azione secondaria.

> **Nota**
> Si consiglia una riparazione automatica, che tuttavia comporta una modifica dei file presenti sul computer da parte di Scanner.

Rinomina

Se l'opzione è attivata, Scanner rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

Quarantena

Se l'opzione è attivata, Scanner sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Elimina

Se l'opzione è attivata, il file viene eliminato. Questa procedura è molto più rapida di **Sovrascrivi ed elimina** (vedere sotto).

Ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

> **Attenzione**
> Il file infetto rimane attivo sul computer. Questo potrebbe causare danni notevoli al computer.

Sovrascrivi ed elimina

Se l'opzione è attivata, Scanner sovrascrive il file con un modello standard, infine lo elimina. Il file non può essere ripristinato.

Azione secondaria

L'opzione "**Azione secondaria**" è selezionabile solo se in "**Azione primaria**" è stata selezionata l'impostazione **Ripara**. Con questa opzione si può decidere come procedere con il file infetto se non è riparabile.

Rinomina

Se l'opzione è attivata, Scanner rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

Quarantena

Se l'opzione è attivata, Scanner sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Elimina

Se l'opzione è attivata, il file viene eliminato. Questa procedura è molto più rapida di "Sovrascrivi ed elimina".

Ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

> **Attenzione**
> Il file infetto rimane attivo sul computer. Questo potrebbe causare danni notevoli al computer.

Sovrascrivi ed elimina

Se l'opzione è attivata, Scanner sovrascrive il file con un modello standard, infine lo elimina. Il file non può essere ripristinato.

> **Nota**
> Se si seleziona **Elimina** o **Sovrascrivi ed elimina** come azione principale o secondaria, attenersi alle seguenti indicazioni: in caso di rilevamento di oggetti euristici, i file infetti non vengono eliminati bensì spostati in quarantena.

Archivi

Per la ricerca negli archivi, Scanner utilizza una scansione ricorsiva: vengono decompressi anche gli archivi in altri archivi e viene controllata la presenza di virus e programmi indesiderati. I file compressi vengono scansionati, decompressi e nuovamente scansionati.

Scansiona archivi

Se l'opzione è attivata, vengono scansionati gli archivi selezionati nell'elenco degli archivi. Questa impostazione è attivata di default.

Tutti i tipi di archivio

Se l'opzione è attivata, vengono selezionati e scansionati tutti i tipi di archivi nell'elenco degli archivi.

Archivio estensioni Smart

Se l'opzione è attivata, Scanner riconosce se un file è in formato compresso (archivio), anche se l'estensione è diversa da quelle abituali, e scansiona l'archivio. Tuttavia a tal fine ogni file deve essere aperto, riducendo così la velocità della scansione. Esempio: se un archivio *.zip ha estensione *.xyz, Scanner decomprime anche tale archivio e lo scansiona. Questa impostazione è attivata di default.

> **Nota**
> Vengono scansionati solo quei tipi di archivio che sono selezionati nell'elenco degli archivi.

Limita la profondità di ricorsione

La decompressione e la scansione di archivi particolarmente ramificati può necessitare di molto tempo e molte risorse del sistema. Se l'opzione è attivata, è possibile limitare la profondità di ricorsione della scansione in archivi multipli a un determinato numero di livelli di compressione (profondità di ricorsione massima). In questo modo è possibile risparmiare tempo e risorse del processore.

> **Nota**
> Per individuare un virus o un programma indesiderato all'interno di un archivio, Scanner deve eseguire la scansione fino al livello di ricorsione nel quale si trova il virus o il programma indesiderato.

Massima profondità di ricorsione

Per poter indicare la profondità massima di ricorsione, l'opzione **Limita la profondità di ricorsione** deve essere attivata.
È possibile inserire direttamente la profondità di ricorsione desiderata oppure modificarla per mezzo dei tasti freccia a destra del campo. I valori consentiti sono compresi tra 1 e 99. Il valore standard e consigliato è 20.

Valori standard

Il pulsante crea i valori predefiniti per la scansione degli archivi.

Elenco archivi

In questa sezione è possibile impostare quali archivi devono essere scansionati da Scanner. A tal fine è necessario selezionare le voci corrispondenti.

Eccezioni

File che Scanner deve tralasciare

L'elenco in questa finestra contiene file e percorsi che non devono essere presi in considerazione da Scanner durante la ricerca di virus e programmi indesiderati.

Si consiglia di inserire quante meno eccezioni possibili e solo i file che non devono essere scansionati durante una scansione normale per qualsivoglia motivo. Consigliamo di far comunque controllare la presenza di virus o programmi indesiderati in questi file prima di inserirli in questo elenco!

Nota
Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Attenzione
Questi file non vengono presi in considerazione durante la scansione!

Nota
I file inseriti in questo elenco vengono segnalati nel file di report. Controllare di tanto in tanto nel file di report la presenza di questi file non scansionati poiché potrebbe non sussistere più il motivo per il quale sono stati esclusi. In questo caso i nomi di questi file dovrebbero essere rimossi dall'elenco.

Campo

Inserire in questo campo il nome del file che non deve essere preso in considerazione durante una scansione diretta. Di default non è indicato alcun file.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file o il percorso desiderato.
Se si è fornito un nome di file con un percorso completo, tale file non viene scansionato. Se si è inserito un nome di file senza un percorso, ogni file con tale nome (indipendentemente dal percorso o dal drive) non verrà scansionato.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nell'elenco. Questo pulsante non è attivo se non è selezionata alcuna voce.

Euristica

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca.

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo programmi di malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei programmi di malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto.

Ciò non significa necessariamente che il codice indichi effettivamente la presenza di malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Il prodotto Avira contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di possibile riparazione vengono eliminate tutte le macro del documento infetto, in alternativa i documenti sospetti vengono solo segnalati e l'utente riceverà un avviso. Questa impostazione è attivata di default ed è consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il programma Avira contiene, grazie alla tecnologia AHeAD di Avira, un'euristica molto efficace, in grado di riconoscere anche programmi di malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di "rigidità" dell'euristica. Questa impostazione è attivata di default.

Livello di riconoscimento basso

Se l'opzione è attivata, viene rilevato un numero inferiore di programmi malware sconosciuti, il rischio di falsi allarmi è limitato.

Livello di riconoscimento medio

Se l'opzione è attivata, viene garantita una protezione bilanciata con pochi messaggi di errore. Questa impostazione è attivata di default se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di programmi di malware sconosciuti, ma possono essere visualizzati messaggi di errore.

10.2.2 Report

Scanner possiede una funzione di log molto ampia. In questo modo si ricevono informazioni esatte sui risultati di una scansione diretta. Il file di report contiene tutte le voci del sistema e gli avvisi e i messaggi della scansione diretta.

> **Nota**
> Per comprendere quali azioni Scanner ha eseguito in caso di rilevamento di virus o programmi indesiderati, deve sempre essere creato un file di report.

Funzione di log

Disabilitato

Se l'opzione è attivata, Scanner non riporta le azioni e i risultati della scansione diretta.

Standard

Se l'opzione è attivata, Scanner riporta il nome dei file infetti con il percorso. Nel file di report vengono riportate inoltre la configurazione per la scansione corrente, le informazioni sulla versione e sul proprietario della licenza.

Avanzato

Se l'opzione è attivata, Scanner riporta anche gli avvisi e le note, oltre alle informazioni standard. Il file di report specifica un suffisso "(cloud)" per identificare gli avvisi del componente Protection Cloud.

Completo

Se l'opzione è attivata, Scanner riporta tutti i file scansionati. Inoltre, tutti i file infetti nonché gli avvisi e le note vengono registrati nel file di report.

Nota
Se l'utente deve inviare un file di report ad Avira (per la ricerca dell'errore), preghiamo di creare il file di report con questa modalità.

10.3 Real-Time Protection

La rubrica Real-Time Protection della configurazione è dedicata alla configurazione della scansione in tempo reale.

10.3.1 Scansione

Solitamente si desidera che il proprio sistema sia costantemente monitorato. A tal fine utilizzare Real-Time Protection (scansione in tempo reale = On-Access-Scanner). In questo modo è possibile ricercare la presenza di virus e programmi indesiderati in tutti i file che vengono aperti o copiati sul computer, "on the fly".

File

Real-Time Protection può utilizzare un filtro per scansionare solamente i file con una determinata estensione (tipo).

Tutti i file

Se l'opzione è attivata, viene eseguita una ricerca di virus e programmi indesiderati in tutti i file indipendentemente dal contenuto e dall'estensione.

Nota
Se **Tutti i file** è attivo, il pulsante **Estensioni file** non è selezionabile.

Utilizza estensioni smart

Se l'opzione è attivata, la selezione dei file da scansionare viene effettuata automaticamente dal programma. Ciò significa che il programma decide in base al contenuto se un file deve essere controllato o meno per la presenza di virus e programmi indesiderati. Questa procedura è lievemente più lenta di **Utilizza l'elenco delle estensioni**, ma molto più sicura poiché i controlli non vengono effettuati solamente sulla base delle estensioni dei file.

Nota
Se **Utilizza estensioni smart** è attivo, il pulsante **Estensioni file** non è selezionabile.

Utilizza l'elenco delle estensioni

Se l'opzione è attivata, vengono scansionati solo i file con una determinata estensione. Sono preimpostati tutti i tipi di file che possono contenere virus e programmi indesiderati. L'elenco può essere modificato manualmente mediante il pulsante "**Estensioni file"**. Questa impostazione è attivata di default ed è consigliata.

Nota
Se questa opzione è attiva e tutte le voci dell'elenco delle estensioni dei file sono state eliminate, viene visualizzato il testo "*Nessuna estensione dei file*" sotto il pulsante **Estensioni file**.

Estensioni file

Con questo pulsante viene richiamata una finestra di dialogo nella quale sono riportate tutte le estensioni dei file che vengono controllate durante una scansione in modalità "**Utilizza l'elenco delle estensioni**". Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o rimuovere voci.

Nota
Prestare attenzione al fatto che l'elenco estensioni dei file può variare da versione a versione.

Drive

Controlla drive di rete

Se l'opzione è attivata, vengono monitorati i file sui drive di rete (drive mappati), come ad esempio volumi sul server, peer drive, ecc.

Nota
Per non compromettere eccessivamente le prestazioni del computer, l'opzione **Controlla drive di rete** dovrebbe essere attivata solo in casi eccezionali.

Attenzione
Se l'opzione è disattivata, i drive di rete **non** vengono monitorati. L'utente non è più protetto da virus e programmi indesiderati!

Nota
Se vengono eseguiti file sui drive di rete, questi vengono scansionati da Real-Time Protection indipendentemente dall'impostazione dell'opzione **Controlla drive di rete**. In alcuni casi i file sui drive di rete vengono scansionati all'apertura, nonostante l'opzione **Controlla drive di rete** sia disattivata. Il motivo: a questi file si accede con l'autorizzazione "Esegui file". Se si desidera escludere dal monitoraggio di Real-Time Protection tali file o anche i file eseguiti, inserire i file nell'elenco dei file da tralasciare (vedi: Eccezioni).

Attiva Caching

Se l'opzione è attivata, i file monitorati sui drive di rete vengono messi a disposizione nella cache di Real-Time Protection. Il monitoraggio dei drive di rete senza funzione di caching è più sicuro, tuttavia è meno efficiente rispetto al monitoraggio dei drive di rete con funzione di caching.

Archivi

Scansiona archivi

Se l'opzione è attivata, vengono scansionati gli archivi. I file compressi vengono scansionati, decompressi e nuovamente scansionati. Questa opzione è disattivata di default. La scansione degli archivi viene limitata dalla profondità di ricorsione, dal numero di file da scansionare e dalle dimensioni dell'archivio. È possibile impostare la profondità di ricorsione massima, il numero di file da scansionare e le dimensioni massime dell'archivio.

Nota
L'opzione è disattivata di default poiché il processo occupa molta memoria. Generalmente si consiglia di scansionare gli archivi con la scansione diretta.

Massima profondità di ricorsione

Per la ricerca negli archivi, Real-Time Protection utilizza una scansione ricorsiva: vengono decompressi anche gli archivi in altri archivi e viene controllata la presenza di virus e programmi indesiderati. L'utente può stabilire la profondità di ricorsione. Il

valore standard per la profondità di ricorsione è 1 ed è quello consigliato: tutti i file che si trovano direttamente nell'archivio principale vengono scansionati.

Numero massimo di file

Per la ricerca negli archivi la scansione viene limitata a un numero massimo di file dell'archivio. Il valore standard per il numero massimo di file da scansionare è 10 ed è quello consigliato.

Dimensione massima (KB)

Per la ricerca negli archivi la scansione viene limitata a una dimensione massima degli archivi da decomprimere. Il valore standard è 1000 KB ed è quello consigliato.

Azione in caso di rilevamento

È possibile definire le azioni che Real-Time Protection deve eseguire quando viene rilevato un virus o un programma indesiderato.

Interattivo

Se l'opzione è attivata, in caso di rilevamento di un virus da parte di Real-Time Protection viene visualizzato un messaggio sul desktop. È possibile rimuovere il malware rilevato oppure richiamare altre azioni possibili per il trattamento del virus selezionando il pulsante "**Dettagli**". Le azioni vengono visualizzate in una finestra di dialogo. Questa opzione è attivata di default.

Ripara

Real-Time Protection ripara i file infetti quando è possibile.

Rinomina

Real-Time Protection rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). Il file può essere riparato successivamente e nuovamente rinominato.

Quarantena

Real-Time Protection sposta il file in quarantena. Il file può essere ripristinato dal Gestore della quarantena se ha un valore informativo oppure, se necessario, inviato ad Avira Malware Research Center. A seconda del file sono disponibili altre possibilità di scelta nel Gestore della quarantena (vedere Gestore della quarantena).

Elimina

Il file viene eliminato. Questa procedura è molto più rapida di **Sovrascrivi ed elimina** (vedere sotto).

Ignora

L'accesso al file viene consentito e il file viene mantenuto.

Sovrascrivi ed elimina

Real-Time Protection sovrascrive il file con un modello standard, infine lo elimina. Il file non può essere ripristinato.

Attenzione
Quando Real-Time Protection è impostato su **Scansione in scrittura**, il file infetto non viene creato.

Standard

Grazie a questo pulsante è possibile selezionare l'azione attivata di default in caso di rilevamento di un virus nella finestra di dialogo. Evidenziare l'azione che deve essere attivata di default e fare clic sul pulsante "**Standard**".

Nota
L'azione **Ripara** non può essere selezionata come azione standard.

È possibile reperire maggiori informazioni qui.

Automatico

Se l'opzione è attivata, in caso di rilevamento di virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. Real-Time Protection reagisce conformemente alle impostazioni definite precedentemente dall'utente in questa sezione.

Copia il file in quarantena prima dell'azione

Se l'opzione è attivata, Real-Time Protection crea una copia di sicurezza (backup) prima dell'esecuzione delle azioni primarie e secondarie desiderate. La copia di sicurezza viene conservata in quarantena. Il file può essere ripristinato dal Gestore della quarantena se ha un valore informativo. Inoltre è possibile inviare la copia di sicurezza ad Avira Malware Research Center. A seconda dell'oggetto sono disponibili altre possibilità di scelta nel Gestore della quarantena (vedere Gestore della quarantena)

Azione primaria

L'azione primaria è l'azione che viene eseguita quando Real-Time Protection rileva un virus o un programma indesiderato. Se l'opzione "**Ripara**" è attiva, ma la riparazione del file infetto non è possibile, verrà eseguita l'azione definita in "**Azione secondaria**".

Nota
L'opzione **Azione secondaria** è selezionabile solo se in **Azione primaria** è stata selezionata l'impostazione **Ripara**.

Ripara

Se l'opzione è attivata, Real-Time Protection ripara automaticamente i file infetti. Se Real-Time Protection non può riparare un file infetto, in alternativa esegue l'opzione selezionata in **Azione secondaria**.

Nota
Si consiglia una riparazione automatica, che tuttavia comporta una modifica dei file presenti sul computer da parte di Real-Time Protection.

Rinomina

Se l'opzione è attivata, Real-Time Protection rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

Quarantena

Se l'opzione è attivata, Real-Time Protection sposta il file nella directory di quarantena. I file in questa directory possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Elimina

Se l'opzione è attivata, il file viene eliminato. Questa procedura è molto più rapida di "Sovrascrivi ed elimina".

Ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer. Questo potrebbe causare danni notevoli al computer.

Sovrascrivi ed elimina

Se l'opzione è attivata, Real-Time Protection sovrascrive il file con un modello standard, infine lo elimina. Il file non può essere ripristinato.

Nega accesso

Se l'opzione è attivata, Real-Time Protection inserisce il rilevamento solo nel file di report se la funzione di report è attivata. Inoltre, Real-Time Protection inserisce una voce nel Log eventi, se questa opzione è attivata.

Attenzione
Quando Real-Time Protection è impostato su **Scansione in scrittura**, il file infetto non viene creato.

Azione secondaria

L'opzione "**Azione secondaria**" è selezionabile solo se in "**Azione primaria**" è stata selezionata l'opzione "**Ripara**". Con questa opzione si può decidere come procedere con il file infetto se non è riparabile.

Rinomina

Se l'opzione è attivata, Real-Time Protection rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

Quarantena

Se l'opzione è attivata, Real-Time Protection sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Elimina

Se l'opzione è attivata, il file viene eliminato. Questa procedura è molto più rapida di "Sovrascrivi ed elimina".

Ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

> **Attenzione**
> Il file infetto rimane attivo sul computer. Questo potrebbe causare danni notevoli al computer.

Sovrascrivi ed elimina

Se l'opzione è attivata, Real-Time Protection sovrascrive il file con un modello standard, infine lo elimina. Il file non può essere ripristinato.

Nega accesso

Se l'opzione è attivata, il file infetto non viene creato. Se la funzione di report è stata attivata, Real-Time Protection inserisce il rilevamento soltanto nel file di report. Inoltre, Real-Time Protection inserisce una voce nel Log eventi, se questa opzione è attivata.

> **Nota**
> Se si seleziona **Elimina** o **Sovrascrivi ed elimina** come azione principale o secondaria, attenersi alle seguenti indicazioni: in caso di rilevamento di oggetti euristici, i file infetti non vengono eliminati bensì spostati in quarantena.

Altre azioni

Utilizza log eventi

Se l'opzione è attivata, a ogni rilevamento viene inserita una voce nel log eventi di Windows. È possibile richiamare gli eventi nel visualizzatore eventi di Windows. Questa impostazione è attivata di default.

Eccezioni

Con queste opzioni è possibile configurare gli oggetti soggetti a eccezioni di Real-Time Protection (scansione in tempo reale). Gli oggetti identificati verranno così esclusi dalla scansione in tempo reale. Real-Time Protection può ignorare gli accessi ai file riportati nell'elenco dei processi da tralasciare durante la scansione in tempo reale. Questa funzione è utile ad esempio per le banche dati o le soluzioni di backup.

Nell'indicare i processi e gli oggetti file da escludere, prestare attenzione a quanto segue: l'elenco viene elaborato dall'alto verso il basso. Più lungo è l'elenco, maggiore è il tempo di cui il processore ha bisogno per elaborare l'elenco a ogni accesso. Si consiglia pertanto di mantenere l'elenco più breve possibile.

Processi che Real-Time Protection deve tralasciare

Tutti gli accessi ai file dei processi indicati in questo elenco vengono ignorati da Real-Time Protection.

Campo

Inserire in questo campo il nome del processo che deve essere ignorato dalla scansione in tempo reale. Di default non è indicato alcun processo.

Il percorso indicato e il nome del file del processo non possono superare i 255 caratteri. È possibile inserire fino a 128 processi. Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Per indicare i processi è possibile utilizzare caratteri Unicode. Pertanto, è possibile indicare nomi di processi o directory che contengono caratteri speciali.

I drive devono essere indicati nel modo seguente: `[lettera del drive]:\`

Il simbolo dei due punti (:) deve essere utilizzato solo per indicare il drive.

Per indicare il processo, è possibile utilizzare la wildcard * (numero a piacere di caratteri) e ? (un unico carattere):

```
C:\Programmi\Applicazioni\applicazione.exe
C:\Programmi\Applicazioni\applicazion?.exe
C:\Programmi\Applicazione\applic*.exe
C:\Programmi\Applicazioni\*.exe
```

Per evitare che l'intero processo venga escluso dal monitoraggio di Real-Time Protection, i dati che contengono esclusivamente i seguenti caratteri non sono validi: * (asterisco), ? (punto interrogativo), / (barra), \ (barra rovesciata), . (punto), : (due punti).

È possibile escludere dal monitoraggio di Real-Time Protection i processi senza percorso completo: `applicazione.exe`

Ciò è valido solo per i processi i cui file eseguibili si trovano sul drive dell'hard disk.

La presenza del percorso completo è necessaria per i processi i cui file eseguibili si trovano su drive collegati, ad esempio i drive di rete. A tale riguardo, prestare

attenzione alle indicazioni di annotazione delle eccezioni relative a drive di rete collegati.

Non indicare alcuna eccezione per i processi i cui file eseguibili si trovano su drive dinamici. I drive dinamici vengono utilizzati per i supporti dati rimovibili, quali CD, DVD o penna USB.

Attenzione
Prestare attenzione al fatto che tutti gli accessi ai file, che vengono avviati da processi e che sono stati evidenziati nell'elenco, sono esclusi dalla scansione di virus e programmi indesiderati!

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare un file eseguibile.

Processi

Il pulsante "**Processi**" apre la finestra "*Selezione del processo*", in cui vengono indicati i processi in corso.

Aggiungi

Con il pulsante è possibile accettare il processo indicato nel campo nella finestra di visualizzazione.

Elimina

Con il pulsante si rimuove un processo selezionato dalla finestra di dialogo.

File che Real-Time Protection deve tralasciare

Tutti gli accessi ai file degli oggetti indicati in questo elenco vengono ignorati da Real-Time Protection.

Campo

Inserire in questo campo il nome del file che deve essere ignorato dalla scansione in tempo reale. Di default non è indicato alcun file.

Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Per indicare i file da tralasciare, è possibile utilizzare la wildcard * (numero a piacere di caratteri) e ? (un unico carattere). È possibile anche escludere singole estensioni di file (incluse le wildcard):

```
C:\directory\*.mdb
*.mdb
*.md?
*.xls*
C:\directory\*.log
```

I nomi delle directory devono concludersi con una barra rovesciata \.

Se una directory viene esclusa, anche tutte le sottodirectory che contiene vengono escluse automaticamente.

Per ogni drive è possibile indicare al massimo 20 eccezioni con il percorso completo (che inizia con la lettera del drive).

Ad es.: `C:\Programmi\Applicazioni\Nome.log`

Il numero massimo di eccezioni senza percorso completo è 64. Ad es.:

`*.log`
`\Processore1\C\Directory1`

In caso di drive dinamici, collegati (montati) come directory a un altro drive, è necessario utilizzare nell'elenco delle eccezioni il nome dell'alias del sistema operativo per il drive collegato:
ad esempio
`\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\`
Anche utilizzando il punto di montaggio stesso (mount point), ad esempio `C:\DynDrive`, si esegue comunque la scansione del drive dinamico. È possibile verificare i nomi dell'alias del sistema operativo dal file di report di Real-Time Protection.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare i file da escludere.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Con il pulsante "Elimina" si rimuove un oggetto file selezionato dalla finestra di visualizzazione.

Per indicare le eccezioni, attenersi alle seguenti indicazioni

Per escludere oggetti anche quando vi si accede con nomi di file DOS brevi (convenzione dei nomi di DOS 8.3), è necessario inserire nell'elenco il nome breve del file corrispondente.

Un nome di file che contiene wildcard non deve concludersi con una barra rovesciata.
Ad esempio:
`C:\Programmi\Applicazione\applic*.exe`
Questa voce non è valida e non viene considerata come un'eccezione!

Attenersi alle seguenti indicazioni in caso di **eccezioni relative a drive di rete collegati**: se si utilizza la lettera del drive di rete collegato, le directory e i file indicati NON vengono

esclusi dalla scansione di Real-Time Protection. Se il percorso UNC nell'elenco delle eccezioni è diverso dal percorso UNC utilizzato per la connessione al drive di rete (indicazione dell'indirizzo IP nell'elenco delle eccezioni – indicazione del nome del computer per la connessione al drive di rete), le directory e i file indicati NON vengono esclusi dalla scansione di Real-Time Protection. Ricavare il percorso UNC da utilizzare in base al file di report di Real-Time Protection:
\\<Nome computer>\<Condivisione>\ - OPPURE- \\<Indirizzo IP>\<Condivisione>\

In base al file di report di Real-Time Protection è possibile verificare i percorsi utilizzati da Real-Time Protection durante la scansione dei file infetti. Nell'elenco delle eccezioni, utilizzare di massima gli stessi percorsi. Procedere come segue: impostare la funzione di log di Real-Time Protection nella configurazione in Report su **Completo**. Accedere, dopo aver attivato Real-Time Protection, a dati, directory, drive collegati o ai drive di rete collegati. È possibile leggere il percorso da utilizzare dal file di report di Real-Time Protection. È possibile richiamare il file di report nel Control Center in Real-Time Protection.

Euristica

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca.

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo programmi di malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei programmi di malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Il prodotto Avira contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di possibile riparazione vengono eliminate tutte le macro del documento infetto, in alternativa i documenti sospetti vengono solo segnalati e l'utente riceverà un avviso. Questa impostazione è attivata di default ed è consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il programma Avira contiene, grazie alla tecnologia AHeAD di Avira, un'euristica molto efficace, in grado di riconoscere anche programmi di malware sconosciuti (nuovi). Se

l'opzione è attivata, è possibile impostare il grado di "rigidità" dell'euristica. Questa impostazione è attivata di default.

Livello di riconoscimento basso

Se l'opzione è attivata, viene rilevato un numero inferiore di programmi malware sconosciuti, il rischio di falsi allarmi è limitato.

Livello di riconoscimento medio

Se l'opzione è attivata, viene garantita una protezione bilanciata con pochi messaggi di errore. Questa impostazione è attivata di default se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di programmi di malware sconosciuti, ma possono essere visualizzati messaggi di errore.

10.3.2 Report

Real-Time Protection possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, Real-Time Protection non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di log, ad esempio solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata, Real-Time Protection registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa impostazione è attivata di default.

Avanzato

Se l'opzione è attivata, Real-Time Protection riporta nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, Real-Time Protection registra tutte le informazioni, anche quelle relative alla dimensione, al tipo di file, alla data ecc., nel file di report.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione indicata di 50 kilobyte, vengono automaticamente eliminate le voci meno recenti fin quando si raggiunge una dimensione inferiore a 50 kilobyte.

Backup file report prima della limitazione

Se l'opzione è attivata, viene eseguito un backup del file di report prima della limitazione.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione utilizzata della scansione in tempo reale viene riportata nel file di report.

Nota
Se non sono state specificate limitazioni per i file di report, viene creato un nuovo file di report quando questo raggiunge le dimensioni di 100 MB. Viene creato un backup del report di dati precedente. Vengono mantenuti fino a tre backup di report di dati precedenti. Vengono eliminati di volta in volta i backup meno recenti.

10.4 Aggiornamento

Nella rubrica **Aggiornamento** è possibile configurare l'esecuzione automatica degli aggiornamenti. È possibile impostare diversi intervalli di aggiornamento,.

Aggiornamento automatico

Ogni n giorni/ore/minuti

In questo campo è possibile indicare l'intervallo in cui devono essere eseguiti gli aggiornamenti automatici. Per modificare l'intervallo di aggiornamento, è possibile indicare un dato temporale nel campo e modificarlo mediante i tasti freccia a destra del campo.

Avvia il job all'avvio della connessione Internet

Se l'opzione è attivata, oltre all'intervallo di aggiornamento stabilito, il job di aggiornamento viene eseguito quando si attiva una connessione a Internet.

Ripeti job se il tempo è scaduto

Se l'opzione è attivata, vengono eseguiti job di aggiornamento scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.

10.4.1 Server Web

Server Web

L'aggiornamento può essere eseguito direttamente mediante server Web in Internet .

Connessione al server Web

Utilizza una connessione esistente (rete)

Questa impostazione viene visualizzata se si utilizza la connessione mediante una rete.

Utilizza la seguente connessione

Questa impostazione viene visualizzata se si definisce individualmente la connessione.

L'Updater riconosce automaticamente quali opzioni di connessione sono disponibili. Le opzioni di connessione non disponibili sono grigie e non possono essere attivate. Ad esempio, è possibile stabilire manualmente una connessione dial-up mediante una voce dell'elenco telefonico di Windows.

Utente

Inserire il nome utente dell'account selezionato.

Password

Inserire la password per questo account. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*).

Nota
Se sono stati dimenticati il nome utente o la password di un account Internet, contattare il provider di servizi Internet.

Nota
La selezione automatica dell'Updater mediante i cosiddetti tool dial-up (ad esempio SmartSurfer, Oleco, ...) attualmente non è ancora disponibile.

Termina nuovamente la connessione dial-up aperta per l'aggiornamento

Se l'opzione è attivata, la connessione dial-up aperta per l'aggiornamento viene interrotta automaticamente non appena il download è stato eseguito con successo.

Nota
L'opzione è disponibile solo in Windows XP. A partire da Windows Vista, la

connessione dial-up aperta per l'aggiornamento viene sempre interrotta al termine del download.

Impostazioni proxy

Server proxy

Non utilizzare un server proxy

Se l'opzione è attivata, la connessione al server Web non viene effettuata mediante un server proxy.

Utilizza impostazioni di sistema di Windows

Se l'opzione è attivata, vengono utilizzate le impostazioni di sistema di Windows correnti per la connessione al server Web mediante un server proxy. Per configurare le impostazioni di sistema di Windows in modo tale che venga utilizzato un server proxy, accedere a **Pannello di controllo > Opzioni Internet > Connessioni > Impostazioni LAN**. Per accedere a Opzioni Internet è possibile utilizzare anche il menu **Strumenti** di Internet Explorer.

Attenzione
Se si utilizza un server proxy che richiede l'autenticazione, specificare tutti i dati in**Utilizza questo server proxy**. L'opzione **Utilizza impostazioni di sistema di Windows** può essere selezionata solo in presenza di server proxy che non richiedono alcuna autenticazione.

Utilizza questo server proxy

Se l'opzione è attivata, la connessione al server Web avviene mediante un server proxy, utilizzando le impostazioni definite dall'utente.

Indirizzo

Immettere il nome del computer o l'indirizzo IP del server proxy che si desidera utilizzare per la connessione al server Web.

Porta

Inserire il numero della porta del server proxy che si desidera utilizzare per la connessione al server Web.

Nome login

Inserire un nome utente per il login al server proxy.

Password login

Inserire la password appropriata per il login al server proxy. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*).

Esempi:

Indirizzo: `proxy.dominio.it` porta: `8080`

Indirizzo: `192.168.1.100` porta: `3128`

10.5 FireWall

10.5.1 Configurazione di FireWall

Avira Ultimate Protection Suite consente di configurare Avira FireWall o Windows Firewall (a partire da Windows 7):

- Windows Firewall

10.5.2 Windows Firewall

La rubrica **FireWall** in **Configurazione > Sicurezza Internet** è dedicata alla configurazione di Windows FireWall nei sistemi operativi a partire da Windows 7.

Profili di rete

Profili di rete

In base ai profili di rete, il Windows FireWall blocca l'accesso al vostro computer da parte di programmi e app non autorizzati:

- Rete privata: per le reti domestiche o dell'ufficio
- Rete pubblica: per le reti pubbliche
- Rete di domini: per le reti con un sistema di controllo dei domini

Potete gestire questi profili dalla configurazione del vostro prodotto Avira, sotto **Sicurezza Internet > Windows FireWall > Profili di rete**.

Per ulteriori informazioni su questi profili di rete, potete visitare il Sito web ufficiale Microsoft.

> **Avviso**
> Windows FireWall applica le stesse regole a tutte le reti appartenenti allo stesso profilo. Ciò significa che se autorizzate un programma o una app, esso ha anche accesso a tutte le reti che utilizzano lo stesso profilo.

Rete privata

Impostazioni di una rete privata

Le impostazioni di una rete privata gestiscono l'accesso di altri computer o apparecchi della vostra rete domestica o dell'ufficio al vostro computer. Queste impostazioni consentono in modo predefinito all'utente della rete privata di visualizzare e accedere al proprio computer.

Abilita

Se l'opzione è attivata, il Windows FireWall si attiva e viene gestito tramite Avira.

Blocca tutte le connessioni in arrivo

Se l'opzione è attiva, tutti i tentativi indesiderati di connessione al vostro computer vengono respinti dal Windows FireWall, a eccezione delle connessioni in entrata provenienti da applicazioni autorizzate.

Inviami una notifica quando una nuova app è bloccata

Se l'opzione è attiva, verrete avvisati ogni volta che una app o un programma viene bloccato.

Desabilita (non consigliato)

Se l'opzione è attivata, il Windows FireWall si disattiva. Questa opzione è sconsigliata, perché potrebbe danneggiare il vostro computer.

Rete pubblica

Impostazioni di una rete pubblica

Le impostazioni di una rete pubblica gestiscono l'accesso di altri computer o apparecchi della rete pubblica al vostro computer. Queste impostazioni non consentono in modo predefinito all'utente della rete pubblica di visualizzare e accedere al proprio computer.

Abilita

Se l'opzione è attivata, il Windows FireWall si attiva e viene gestito tramite Avira.

Blocca tutte le connessioni in arrivo

Se l'opzione è attiva, tutti i tentativi indesiderati di connessione al vostro computer vengono respinti dal Windows FireWall, a eccezione delle connessioni in entrata provenienti da applicazioni autorizzate.

Inviami una notifica quando una nuova app è bloccata

Se l'opzione è attiva, verrete avvisati ogni volta che una app o un programma viene bloccato.

Desabilita (non consigliato)

Se l'opzione è attivata, il Windows FireWall si disattiva. Questa opzione è sconsigliata, perché potrebbe danneggiare il vostro computer.

Rete di domini

Impostazioni di una rete di domini

Le impostazioni di una rete di domini gestiscono l'accesso di altri computer o apparecchi al vostro computer, se il vostro computer è collegato a una rete autentificata tramite un sistema di controllo dei domini. Queste impostazioni consentono in modo predefinito all'utente autentificato dei domini di visualizzare e accedere al proprio computer.

Abilita

Se l'opzione è attivata, il Windows FireWall si attiva e viene gestito tramite Avira.

Blocca tutte le connessioni in arrivo

Se l'opzione è attivata, tutti i tentativi indesiderati di connessione al vostro computer vengono respinti dal Windows FireWall, a eccezione delle connessioni in entrata provenienti da applicazioni autorizzate.

Inviami una notifica quando una nuova app è bloccata

Se l'opzione è attiva, verrete avvisati ogni volta che una app o un programma viene bloccato.

Desabilita (non consigliato)

Se l'opzione è attivata, il Windows FireWall si disattiva. Questa opzione è sconsigliata, perché potrebbe danneggiare il vostro computer.

> **Nota**
> questa opzione è disponibile solo qualora il vostro computer sia connesso a una rete che dispone di un sistema di controllo dei domini.

Regole di applicazione

Se cliccate sul link sotto **Windows FireWall > Regole di applicazione** , venite inoltrati al menu **App e funzionalità consentite** della configurazione Windows FireWall.

Impostazioni avanzate

Se cliccate sul link sotto **Windows FireWall > Impostazioni avanzate** , venite inoltrati al menu **Windows FireWall con sicurezza avanzata** della configurazione Windows FireWall.

10.6 Web Protection

La rubrica **Web Protection** in **Configurazione > Sicurezza Internet** è dedicata alla configurazione di Web Protection.

10.6.1 Scansione

Web Protection consente la protezione da virus e malware che giungono sul computer attraverso i siti Web caricati da Internet nel browser Web. Nella rubrica **Scansione** è possibile impostare il comportamento di Web Protection.

Scansione

Supporto di IPv6

Se l'opzione è attivata, viene supportata la versione 6 del protocollo Internet di Web Protection. Questa opzione non è disponibile per nuove installazioni o per modifiche all'installazione di Windows 8.

Protezione Drive-by

La *protezione Drive-by* consente di effettuare impostazioni per bloccare gli iframe, detti anche inline frame. Gli iframe sono elementi HTML, ovvero elementi di siti Internet, che delimitano un'area di un sito Web. Gli iframe consentono di caricare e visualizzare altri contenuti Web, per lo più di altri URL, come documenti indipendenti in una sottofinestra del browser. Gli iframe vengono principalmente utilizzati per i banner pubblicitari. In alcuni casi gli iframe vengono utilizzati per nascondere virus e malware. In questi casi l'area dell'iframe nel browser è appena o per niente visibile. L'opzione **Blocca iframe sospetti** consente di controllare e di bloccare il caricamento di iframe.

Blocca iframe sospetti

Se l'opzione è attivata, gli iframe dei siti Web richiesti vengono verificati in base a determinati criteri. Se in uno dei siti Web richiesti sono presenti iframe sospetti, l'iframe viene bloccato. Nella finestra dell'iframe viene visualizzato un messaggio d'errore.

Azione in caso di rilevamento

È possibile stabilire delle azioni che Web Protection deve eseguire quando viene rilevato un virus o un programma indesiderato.

Interattivo

Se l'opzione è attivata, durante la scansione diretta in caso di rilevamento di un virus o di un programma indesiderato appare una finestra di dialogo nella quale è possibile scegliere come procedere con i file infetti. Questa impostazione è attivata di default.

Visualizza barra di progressione

Se l'opzione è attivata, quando un download o lo scaricamento del contenuto di pagine Web supera un timeout di 20 secondi viene visualizzato un messaggio sul desktop con una barra di progressione per il download. Questo messaggio sul desktop è utile in particolare per il controllo del download da pagine Web con grandi volumi di dati: navigando con Web Protection i contenuti delle pagine Web non vengono caricati gradualmente nel browser Internet poiché, prima di essere visualizzati nel browser

Internet, vengono scansionati alla ricerca di virus e malware. Questa opzione è disattivata di default.

È possibile reperire maggiori informazioni qui.

Automatico

Se l'opzione è attivata, in caso di rilevamento di virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. Web Protection reagisce conformemente alle impostazioni definite in questa sezione.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando Web Protection rileva un virus o un programma indesiderato.

Nega accesso

Il sito Web richiesto dal server Web o i dati e i file trasferiti non vengono inviati al proprio browser Web. Nel browser Web viene visualizzato un messaggio di errore relativo al divieto di accesso. Web Protection inserisce il rilevamento nel file di report, a condizione che la funzione di report sia attivata.

Sposta in quarantena

Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inviati in quarantena in caso di rilevamento di un virus o di malware. Il file infetto può essere ripristinato dal Gestore della quarantena se ha un valore informativo, oppure, se necessario, inviato ad Avira Malware Research Center.

Ignora

Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inoltrati da Web Protection al proprio browser Web. L'accesso al file viene consentito e il file viene mantenuto.

> **Attenzione**
> Il file infetto rimane attivo sul computer. Questo potrebbe causare danni notevoli al computer.

Accessi bloccati

In **Accessi bloccati** è possibile immettere i tipi di file e i tipi MIME (tipi di contenuto dei dati trasmessi) che devono essere bloccati da Web Protection. Il filtro Web consente di bloccare URL noti indesiderati, quali gli URL di phishing e malware. Web Protection impedisce il trasferimento dei file da Internet al computer.

Tipi di file / MIME che Web Protection deve bloccare

Tutti i tipi di file e i tipi MIME (tipo di contenuto dei dati trasmessi) nell'elenco vengono bloccati da Web Protection.

Campo

In questo campo immettere i nomi dei tipi MIME e dei tipi di file che devono essere bloccati da Web Protection. Per i tipi di file inserire l'estensione del file, ad esempio **.htm**. Per i MIME segnalare il tipo di supporto ed eventualmente il sottotipo. I due dati vengono separati da una semplice barra, ad esempio **video/mpeg** o **audio/x-wav**.

Nota
I file che sono già stati salvati come file Internet temporanei sul computer vengono sicuramente bloccati da Web Protection, ma possono comunque essere caricati dal browser Internet locale dal computer. I file temporanei Internet sono file che vengono memorizzati sul computer dal browser Internet per poter visualizzare le pagine Web più rapidamente.

Nota
L'elenco dei tipi di file e dei tipi MIME da bloccare viene ignorato per le voci dell'elenco dei tipi di file e dei tipi MIME da tralasciare in Eccezioni.

Nota
Nell'immissione dei tipi di file e di MIME non è possibile utilizzare wildcard (wildcard * per un numero a piacere di caratteri o ? per un solo carattere).

Tipi MIME: esempi per tipi di supporto

- `text` = per file di testo
- `image` = per file di grafica
- `video` = per file video
- `audio` = per file audio
- `application` = per file associati a un programma specifico

Esempi: tipi di file e di MIME da escludere

- `application/octet-stream` = i file del tipo MIME application/octet-stream (eseguibili *.bin, *.exe, *.com, *dll, *.class) vengono bloccati da Web Protection.
- `application/olescript` = i file del tipo MIME application/olescript (file di script ActiveX *.axs) vengono bloccati da Web Protection.
- `.exe` = tutti i file con l'estensione .exe (file eseguibili) vengono bloccati da Web Protection.
- `.msi` = tutti i file con estensione .msi (Windows Installer) vengono bloccati da Web Protection.

Aggiungi

Con il pulsante è possibile accettare il tipo di MIME o di file immesso nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nell'elenco. Questo pulsante non è attivo se non è selezionata alcuna voce.

Filtro Web

Il filtro Web dispone di una banca dati interna aggiornata quotidianamente nella quale gli URL sono classificati in base a criteri di contenuto.

Attiva filtro Web

Se l'opzione è attivata, vengono bloccati tutti gli URL appartenenti alle categorie selezionate nell'elenco del filtro Web.

Elenco filtro Web

Nell'elenco del filtro Web è possibile selezionare le categorie di contenuto i cui URL devono essere bloccati da Web Protection.

> **Nota**
> Il filtro Web viene ignorato per le voci dell'elenco degli URL da tralasciare in Eccezioni.

> **Nota**
> Vengono categorizzati come **URL di spam** gli URL diffusi con i messaggi e-mail di spam. La categoria **Frode / Inganno** comprende i siti Web con "abbonamenti trappola" e altre offerte di servizi i cui costi vengono occultati dal fornitore.

Eccezioni

Queste opzioni consentono di escludere tipi di MIME (tipi di contenuto dei file trasferiti) e tipi di file per gli URL (indirizzi Internet) dalla scansione di Web Protection. Gli URL e i tipi di MIME indicati vengono ignorati da Web Protection, ovvero durante la trasmissione al computer dell'utente non viene effettuata la scansione di questi dati per verificare la presenza di virus e malware.

Tipi MIME che Web Protection deve tralasciare

In questo campo è possibile selezionare tipi MIME (tipi di contenuto dei dati trasferiti) che devono essere esclusi dalla scansione di Web Protection.

Tipi di file / tipi MIME (personalizzati) che Web Protection deve tralasciare

Tutti i tipi di file e i tipi MIME (tipi di contenuto dei dati trasferiti) nella lista vengono esclusi dalla scansione di Web Protection.

Campo

Inserire in questo campo i nomi dei tipi MIME e i tipi di dati che si intendono escludere dalla scansione di Web Protection. Per i tipi di file inserire l'estensione del file, ad esempio `.htm`. Per i MIME segnalare il tipo di supporto ed eventualmente il sottotipo. I due dati vengono separati da una semplice barra, ad esempio `video/mpeg` o `audio/x-wav`.

> **Nota**
> Nell'immissione dei tipi di file e di MIME non è possibile utilizzare wildcard (wildcard * per un numero a piacere di caratteri o ? per un solo carattere).

> **Attenzione**
> Tutti i tipi di file e di contenuto nell'elenco delle eccezioni vengono caricati nel browser Internet senza ulteriori verifiche di blocco dell'accesso (elenco dei tipi di file e di MIME da bloccare in Accessi bloccati) o di Web Protection: per tutte le voci dell'elenco delle eccezioni viene ignorato il contenuto dell'elenco dei tipi di file e di MIME da bloccare. Non viene eseguita alcuna scansione per virus e malware.

Tipi MIME: esempi per tipi di supporto

- `text` = per file di testo
- `image` = per file di grafica
- `video` = per file video
- `audio` = per file audio
- `application` = per file associati a un programma specifico

Esempi: tipi di file e di MIME da escludere

- `audio/` = tutti i file del tipo supporto audio vengono esclusi dalla scansione di Web Protection
- `video/quicktime` = tutti i file video di sottotipo Quicktime (*.qt, *.mov) vengono esclusi dalla scansione di Web Protection
- `.pdf` = tutti i file Adobe-PDF vengono esclusi dalla scansione di Web Protection.

Aggiungi

Con il pulsante è possibile accettare il tipo di MIME o di file immesso nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nell'elenco. Questo pulsante non è attivo se non è selezionata alcuna voce.

URL che Web Protection deve tralasciare

Tutti gli URL di questo elenco vengono esclusi dalla scansione di Web Protection.

Campo

Immettere in questo campo gli URL (indirizzi Internet) che devono essere esclusi dalla scansione di Web Protection, ad esempio **www.domainname.com**. È possibile inserire parti di URL definendo il livello del dominio con punti iniziali o finali: .domainname.it per tutte le pagine e tutti i domini secondari del dominio. Per indicare una pagina Web con un dominio di livello superiore a piacere (.com o .net), utilizzare un punto finale: **domainname.**. Se si utilizza una sequenza di caratteri senza punto iniziale o finale, viene interpretata come dominio di livello superiore, ad es. **net** per tutti i domini NET (www.domain.net).

Nota
Nell'immissione degli URL è possibile utilizzare anche wildcard * per un numero di caratteri a piacere. Per definire il livello del dominio, utilizzare anche punti iniziali o finali in combinazione con wildcard:
`.domainname.*`
`*.domainname.com`
`.*name*.com` (valido ma non consigliato)
Le immissioni senza punti quali `*name*` vengono interpretati come parti di dominio di livello superiore e non sono consigliati.

Attenzione
Tutti i siti Web dell'elenco degli URL da escludere vengono caricati nel browser Internet senza ulteriori verifiche del filtro Web o di Web Protection: per tutte le voci dell'elenco degli URL da tralasciare vengono ignorate le voci del filtro Web (vedere Accessi bloccati). Non viene eseguita alcuna scansione per virus e malware. Si consiglia pertanto di escludere dalla scansione di Web Protection solo URL affidabili.

Aggiungi

Con il pulsante è possibile accettare gli URL (indirizzi Internet) inseriti nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nell'elenco. Questo pulsante non è attivo se non è selezionata alcuna voce.

Esempi: URL da tralasciare

- `www.avira.com` -OPPURE- `www.avira.com/*`
  = tutti gli URL con il dominio "www.avira.com" vengono esclusi dalla scansione di Web Protection: www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,... Gli URL con dominio www.avira.it vengono esclusi dalla scansione di Web Protection.
- `avira.com` -OPPURE- `*.avira.com`
  = tutti gli URL con dominio di livello secondario o superiore "avira.com" vengono esclusi dalla scansione di Web Protection. Tali dati comprendono tutti i domini secondari esistenti di "avira.com": www.avira.com, forum.avira.com,...
- `avira.` -OPPURE- `*.avira.*`
  = tutti gli URL con dominio di livello secondario "avira" vengono esclusi dalla scansione di Web Protection. Tali dati comprendono tutti i domini esistenti di livello superiore o i domini secondari di ".avira.": www.avira.com, www.avira.de, forum.avira.com,...
- `.*domain*.*`
  = tutti gli URL che contengono un dominio di livello secondario con la sequenza di caratteri "domain" vengono esclusi dalla scansione di Web Protection: www.domain.com, www.new-domain.it, www.sample-domain1.it, ...
- `net` -OPPURE- `*.net`
  = tutti gli URL con dominio di livello superiore "net" vengono esclusi dalla scansione di Web Protection: www.name1.net, www.name2.net,...

Attenzione
Indicare tutti gli URL che si desidera escludere dalla scansione di Web Protection in modo più preciso possibile. Evitare l'immissione di tutti i domini di livello superiore o parti di nomi di domini secondari, poiché vi è il rischio che le pagine Internet, che diffondono malware e programmi indesiderati mediante dati globali, vengano escluse dalla scansione di Web Protection come eccezione. Si consiglia di immettere almeno il dominio secondario e il dominio di livello superiore completi: domainname.com

Euristica

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca.

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo programmi di malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei programmi di malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere

con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Il prodotto Avira contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di possibile riparazione vengono eliminate tutte le macro del documento infetto, in alternativa i documenti sospetti vengono solo segnalati e l'utente riceverà un avviso. Questa impostazione è attivata di default ed è consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il prodotto Avira contiene, grazie alla tecnologia AHeAD di Avira, un'euristica molto efficace, in grado di riconoscere anche programmi di malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di "rigidità" dell'euristica. Questa impostazione è attivata di default.

Livello di riconoscimento basso

Se l'opzione è attivata, viene rilevato un numero inferiore di programmi malware sconosciuti, il rischio di falsi allarmi è limitato.

Livello di riconoscimento medio

Se l'opzione è attivata, viene garantita una protezione bilanciata con pochi messaggi di errore. Questa impostazione è attivata di default se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di programmi di malware sconosciuti, ma possono essere visualizzati messaggi di errore.

10.6.2 Report

Web Protection possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, Web Protection non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di log, ad esempio solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata Web Protection registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, le informazioni meno importanti vengono ignorate per una sintesi migliore. Questa impostazione è attivata di default.

Avanzato

Se l'opzione è attivata, Web Protection riporta nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, Web Protection registra tutte le informazioni, anche quelle relative alla dimensione, al tipo di file, alla data ecc., nel file di report.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione indicata di 50 kilobyte, vengono automaticamente eliminate le voci meno recenti fin quando si raggiunge una dimensione inferiore del 20%.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione utilizzata della scansione in tempo reale viene riportata nel file di report.

Nota
Se non sono state specificate limitazioni per i file di report, vengono automaticamente eliminate le voci più vecchie quando il file di report raggiunge le dimensioni di 100 MB. Viene eliminato un numero di voci tali da consentire al file di report di raggiungere una dimensione di 80 MB.

10.7 Mail Protection

La rubrica Mail Protection della configurazione è dedicata alla configurazione di Mail Protection.

10.7.1 Scansione

Mail Protection viene utilizzato per verificare la presenza di virus, malware nelle e-mail in ingresso. Nelle e-mail in uscita, Mail Protection verifica la presenza di virus e malware. Le e-mail in uscita, inviate da un Bot sconosciuto per la diffusione di spam sul computer dell'utente, possono essere bloccate da Mail Protection.

Scansione e-mail in entrata

Se l'opzione è attivata, nelle e-mail in entrata viene verificata la presenza di virus, malware. Mail Protection supporta i protocolli POP3 e IMAP. Attivare l'account di posta in entrata, utilizzato dal client e-mail dell'utente per ricevere le e-mail, per il monitoraggio mediante Mail Protection.

Controlla account POP3

Se l'opzione è attivata, gli account POP3 vengono monitorati alle porte indicate.

Porte controllate

Immettere nel campo la porta utilizzata dal protocollo POP3 per la posta in entrata. Più porte vengono indicate separate da una virgola.

Standard

Il pulsante consente di reimpostare le porte indicate sulla porta standard di POP3.

Controlla account IMAP

Se l'opzione è attivata, gli account IMAP vengono controllati alle porte indicate.

Porte controllate

Immettere nel campo la porta utilizzata dal protocollo IMAP. Più porte vengono indicate separate da una virgola.

Standard

Il pulsante consente di reimpostare le porte indicate sulla porta standard di IMAP.

Scansiona e-mail in uscita (SMTP)

Se l'opzione è attivata, nelle e-mail in uscita viene verificata la presenza di virus e malware. Le e-mail inviate da Bot sconosciuti per la diffusione di spam vengono bloccate.

Porte controllate

Immettere nel campo la porta utilizzata per la posta in uscita dal protocollo SMTP. Più porte vengono indicate separate da una virgola.

Standard

Il pulsante consente di reimpostare le porte indicate sulla porta standard di SMTP.

Nota
Per verificare le porte e i protocolli utilizzati, richiamare le proprietà degli account di posta elettronica nel programma e-mail client utilizzato. Vengono principalmente utilizzate porte standard.

Supporto di IPv6

Se l'opzione è attivata, viene supportata la versione 6 del protocollo Internet di Mail Protection. L'opzione non è disponibile per nuove installazioni o per modifiche di installazione di Windows 8.

Azione in caso di rilevamento

Questa rubrica di configurazione contiene le impostazioni delle azioni da intraprendere quando Mail Protection rileva un virus o un programma indesiderato in un'e-mail o in un allegato.

> **Nota**
> Le azioni definite qui vengono eseguite sia in caso di rilevamento di un virus nelle e-mail in ingresso che nelle e-mail in uscita.

Interattivo

Se l'opzione è attivata, in caso di rilevamento di un virus o di un programma indesiderato in un'e-mail o in un allegato appare una finestra di dialogo nella quale si può selezionare come procedere con l'e-mail o con l'allegato infetto. Questa opzione è attivata di default.

Visualizza barra di progressione

Se l'opzione è attivata, durante il download delle e-mail Mail Protection visualizza una barra di progressione. È possibile attivare questa opzione solo se è stata selezionata l'opzione **Interattivo**.

Automatico

Se l'opzione è attivata, non viene più segnalato il rilevamento di un virus o di un programma indesiderato. Mail Protection reagisce conformemente alle impostazioni definite in questa sezione.

E-mail infette

L'opzione selezionata in "*E-mail infette*" verrà eseguita come azione primaria quando Mail Protection rileva un virus o un programma indesiderato in un'e-mail. Se è stata selezionata l'opzione "**Ignora**", in "*Allegati infetti*" è possibile scegliere come procedere in caso di un rilevamento in un allegato.

Elimina

Se l'opzione è attivata, l'e-mail infetta viene automaticamente eliminata in caso di rilevamento di un virus o di un programma indesiderato. Il corpo dell'e-mail (body) viene sostituito dal testo standard indicato di seguito. Lo stesso vale per gli allegati (attachment); anche questi ultimi vengono sostituiti da un testo standard.

Ignora

Se l'opzione è attivata, l'e-mail infetta viene ignorata nonostante il rilevamento di un virus o di un programma indesiderato. Si ha tuttavia la possibilità di decidere come procedere con un allegato infetto.

Sposta in quarantena

Se l'opzione è attivata, l'e-mail completa, inclusi gli allegati, viene collocata in quarantena in caso di rilevamento di virus e programmi indesiderati. Successivamente, se lo si desidera, può essere ripristinata. Le e-mail infette vengono eliminate. Il corpo dell'e-mail (body) viene sostituito dal testo standard indicato di seguito. Lo stesso vale per gli allegati (attachment); anche questi ultimi vengono sostituiti da un testo standard.

Allegati infetti

L'opzione "**Allegati infetti**" è selezionabile solo se in "*E-mail infette*" è stata selezionata l'impostazione "**Ignora**". Con questa opzione si può decidere come procedere in caso di rilevamento in un allegato.

Elimina

Se l'opzione è attivata, in caso di rilevamento di un virus o di un programma indesiderato, l'allegato infetto viene eliminato e sostituito con un testo standard.

Ignora

Se l'opzione è attivata, l'allegato infetto viene ignorato e inoltrato nonostante il rilevamento di un virus o di un programma indesiderato.

Attenzione
Se si seleziona questa opzione non si gode di alcuna protezione da parte di Mail Protection contro virus e programmi indesiderati. Effettuare questa scelta solo se si è sicuri di quello che si sta facendo. Disattivare l'anteprima nel programma di posta elettronica, non aprire mai gli allegati facendo doppio clic.

Sposta in quarantena

Se l'opzione è attivata, l'allegato infetto viene collocato in quarantena e infine eliminato (sostituito con un testo standard). Successivamente, se lo si desidera, l'allegato può essere ripristinato.

Altre azioni

Questa rubrica di configurazione contiene ulteriori impostazioni relative alle azioni da intraprendere quando Mail Protection rileva un virus o un programma indesiderato in un'e-mail o in un allegato.

> **Nota**
> Le azioni qui impostate vengono eseguite solo se viene rilevato un virus nelle e-mail in ingresso.

Testo standard per e-mail cancellate e spostate

Il testo in questo campo viene aggiunto come notifica all'e-mail in sostituzione dell'e-mail infetta. Tale messaggio è modificabile. Può contenere un numero massimo di 500 caratteri.

Per la formattazione si possono utilizzare le seguenti combinazioni di tasti:

Ctrl + Invio = inserisce un'interruzione di riga.

Standard

Il pulsante inserisce un testo standard predefinito nel campo.

Testo standard per allegati cancellati e spostati

Il testo in questo campo viene aggiunto come notifica all'e-mail in sostituzione dell'allegato infetto. Tale messaggio è modificabile. Può contenere un numero massimo di 500 caratteri.

Per la formattazione si possono utilizzare le seguenti combinazioni di tasti:

Ctrl + Invio = inserisce un'interruzione di riga.

Standard

Il pulsante inserisce un testo standard predefinito nel campo.

Euristica

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca.

I prodotti Avira contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo programmi di malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei programmi di malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Il prodotto Avira contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di possibile riparazione vengono eliminate tutte le macro del

documento infetto, in alternativa i documenti sospetti vengono solo segnalati e l'utente riceverà un avviso. Questa impostazione è attivata di default ed è consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il prodotto Avira contiene, grazie alla tecnologia AHeAD di Avira, un'euristica molto efficace, in grado di riconoscere anche programmi di malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di "rigidità" dell'euristica. Questa impostazione è attivata di default.

Livello di riconoscimento basso

Se l'opzione è attivata, viene rilevato un numero inferiore di programmi malware sconosciuti, il rischio di falsi allarmi è limitato.

Livello di riconoscimento medio

Se l'opzione è attivata, viene garantita una protezione bilanciata con pochi messaggi di errore. Questa impostazione è attivata di default se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di programmi di malware sconosciuti, ma possono essere visualizzati messaggi di errore.

AntiBot

La funzione AntiBot di Mail Protection consente di evitare che il computer venga sfruttato per la diffusione di e-mail di spam all'interno di una cosiddetta Bot-Net: per la diffusione di spam tramite una Bot-Net, di norma un aggressore infetta diversi computer con un bot, che si collega a un server IRC, utilizza un canale specifico e qui attende il comando di invio delle e-mail di spam. Per differenziare le e-mail di spam di un bot sconosciuto da quelle dell'utente, Mail Protection verifica se il server SMTP utilizzato e il mittente dell'e-mail in uscita si trovano nell'elenco dei server e dei mittenti autorizzati. In caso contrario, l'e-mail in uscita viene bloccata, ovvero non viene inviata. L'e-mail bloccata viene segnalata in una finestra di dialogo.

> **Nota**
> La funzione AntiBot può essere utilizzata solo se la scansione di Mail Protection è attiva per le e-mail in uscita (vedere l'opzione **Scansiona e-mail in uscita** in Mail Protection > Scansione).

Server autorizzati

Tutti i server in questo elenco sono autorizzati da Mail Protection all'invio di e-mail: le e-mail inviate a questi server **non** vengono bloccate da Mail Protection. Se l'elenco non contiene alcun server, nelle e-mail in uscita non viene verificato il server SMTP utilizzato.

Se l'elenco contiene voci, Mail Protection blocca le e-mail inviate a un server SMTP non presente nell'elenco.

Campo

In questo campo vengono immessi il nome host o l'indirizzo IP del server SMTP utilizzato per l'invio delle e-mail.

> **Nota**
> I dati relativi ai server SMTP utilizzati dal programma e-mail per l'invio delle e-mail sono riportati all'interno del programma e-mail nei dati dell'account utente impostati.

Aggiungi

Il pulsante consente di aggiungere il server inserito nel campo all'elenco dei server autorizzati.

Elimina

Il pulsante elimina una voce selezionata dall'elenco dei server autorizzati. Questo pulsante non è attivo se non è selezionata alcuna voce.

Elimina tutti

Il pulsante elimina tutte le voci dell'elenco dei server autorizzati.

Mittenti autorizzati

Tutti i mittenti in questo elenco sono autorizzati da Mail Protection all'invio di e-mail: le e-mail inviate da questi indirizzi e-mail **non** vengono bloccate da Mail Protection. Se l'elenco non contiene alcun mittente, nelle e-mail in uscita non viene verificato l'indirizzo e-mail del mittente. Se l'elenco contiene delle voci, Mail Protection blocca le e-mail inviate da mittenti non presenti nell'elenco.

Campo

In questo campo immettere gli indirizzi e-mail dei mittenti.

Aggiungi

Il pulsante consente di accettare il mittente inserito nel campo nell'elenco dei mittenti autorizzati.

Elimina

Il pulsante elimina una voce selezionata dall'elenco dei mittenti autorizzati. Questo pulsante non è attivo se non è selezionata alcuna voce.

Elimina tutti

Il pulsante elimina tutte le voci dall'elenco dei mittenti autorizzati.

10.7.2 Generale

Eccezioni

Indirizzi Email non verificati

Questa tabella mostra l'elenco di indirizzi Email esclusi dalla scansione di Avira Mail Protection (whitelist).

> **Nota**
> L'elenco delle eccezioni viene utilizzato da Mail Protection esclusivamente per le email in ingresso.

Indirizzi Email non verificati

Campo

Inserire in questo campo gli indirizzi email che si desidera aggiungere all'elenco degli indirizzi Email da non controllare. L'indirizzo Email non verrà più controllato da Mail Protection in futuro, in base alle impostazioni dell'utente.

Aggiungi

Con questo pulsante è possibile aggiungere all'elenco degli indirizzi Email da non verificare un indirizzo Email indicato nel campo.

Elimina

Questo pulsante permette di eliminare dall'elenco un indirizzo Email selezionato.

Indirizzo Email

Indirizzo Email che non deve più essere scansionato.

Malware

Se l'opzione è attivata, l'indirizzo Email non viene più verificata la presenza di malware.

In alto

Questo pulsante consente di spostare un indirizzo Email selezionato in una posizione superiore. Il pulsante non è attivo se non è selezionata alcuna voce o se l'indirizzo selezionato si trova già nella prima posizione dell'elenco.

In basso

Questo pulsante consente di spostare un indirizzo Email selezionato in una posizione inferiore. Il pulsante non è attivo se non è selezionata alcuna voce o se l'indirizzo selezionato si trova già nell'ultima posizione dell'elenco.

Memoria temporanea

La memoria temporanea di Mail Protection contiene i dati relativi alle e-mail scansionate che vengono visualizzati nella statistica del Control Center in **Mail Protection**.

Numero massimo di e-mail nella memoria temporanea

In questo campo viene indicato il numero massimo di e-mail che Mail Protection conserva nella memoria temporanea. Vengono eliminate di volta in volta le e-mail meno recenti.

Memorizzazione massima di un'e-mail in giorni

In questo campo viene inserita la durata massima della memorizzazione di un'e-mail in giorni. Dopo questo periodo, l'e-mail viene eliminata dalla memoria temporanea.

Svuota memoria temporanea

Facendo clic sul pulsante vengono eliminate le e-mail conservate nella memoria temporanea.

Piè di pagina

In **Piè di pagina** è possibile configurare un piè di pagina che verrà visualizzato nelle e-mail inviate dall'utente.

Il presupposto per questa funzione è l'attivazione del controllo con Mail Protection delle e-mail in uscita; vedere l'opzione **Scansiona e-mail in uscita (SMTP)** in **Configurazione > Mail Protection > Scansione**. È possibile utilizzare il piè di pagina definito di Avira Mail Protection con il quale si conferma che l'e-mail inviata è stata controllata da un programma antivirus. È anche possibile immettere un testo per un piè di pagina personalizzato. Se vengono utilizzate entrambe le opzioni come piè di pagina, il testo personalizzato viene anteposto al piè di pagina di Avira Mail Protection.

Piè di pagina nelle e-mail da inviare

Allega piè di pagina Mail Protection

Se l'opzione è attivata, il piè di pagina di Avira Mail Protection viene visualizzato nel testo del messaggio delle e-mail inviate. Con il piè di pagina di Avira Mail Protection si conferma che l'e-mail inviata è stata controllata da Avira Mail Protection per verificare la presenza di virus e programmi indesiderati e che l'e-mail non proviene da un bot sconosciuto. Il piè di pagina di Avira Mail Protection contiene il testo seguente: "*Scansionato con Avira Mail Protection [versione del prodotto] [abbreviazione del*

nome e numero versione del motore di ricerca] [abbreviazione del nome e numero versione del file di definizione dei virus]".

Allega questo piè di pagina

Se l'opzione è attivata, il testo indicato nel campo viene visualizzato come piè di pagina.

Campo

In questo campo è possibile immettere un testo che viene visualizzato come piè di pagina nelle e-mail inviate.

10.7.3 Report

Mail Protection possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, Mail Protection non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di log, ad esempio solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata, Mail Protection registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, le informazioni meno importanti vengono ignorate per una sintesi migliore. Questa impostazione è attivata di default.

Avanzato

Se l'opzione è attivata, Mail Protection riporta nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, Mail Protection registra nel file di report tutte le informazioni.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione indicata di 50 kilobyte, vengono

automaticamente eliminate le voci meno recenti fin quando si raggiunge una dimensione inferiore a 50 kilobyte.

Backup file report prima della limitazione

Se l'opzione è attivata, viene eseguito un backup del file di report prima della limitazione.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione utilizzata di Mail Protection viene scritta nel file del report.

> **Nota**
> Se non sono state specificate limitazioni per i file di report, viene creato un nuovo file di report quando questo raggiunge le dimensioni di 100 MB. Viene creato un backup del report di dati precedente. Vengono mantenuti fino a tre backup di report di dati precedenti. Vengono eliminati di volta in volta i backup meno recenti.

10.8 Safe Browsing

Se è stata assegnata una password per la funzione **Safe Browsing**, la configurazione di **Safe Browsing** viene nascosta e viene visualizzato il pulsante **Protetto da password**.

Protetto da password

Premere il pulsante "**Protetto da password**" e inserire la password per "**Safe Browsing**" nella finestra "**Inserimento password**" per abilitare la configurazione di **Safe Browsing**.

Attiva Safe Browsing

Se l'opzione è attivata, tutti i siti Web richiesti durante la navigazione in Internet vengono verificati in base al ruolo che è stato assegnato all'utente registrato in **Safe Browsing**. I siti Web richiesti vengono bloccati se sono stati classificati come non consentiti nell'ambito del ruolo assegnato.

> **Nota**
> Se **Safe Browsing** è attivato, l'utente del computer al quale non è stato assegnato alcun ruolo nella configurazione della funzione **Safe Browsing** viene classificato di default dal programma come *Standard* con il ruolo **Bambino**. È possibile modificare il ruolo dell'utente standard.
> Dopo l'installazione vengono applicati i ruoli utente **Bambino**, **Adolescente** e **Adulto**. Nei ruoli preconfigurati, la limitazione temporale dell'utilizzo di Internet è disattivata.

Selezione utente

Utente

L'elenco contiene tutti gli utenti del sistema.

Aggiungi

Il pulsante consente di aggiungere l'utente selezionato all'elenco degli utenti protetti.

Elimina

Il pulsante consente di eliminare la voce dell'elenco selezionata.

Elenco "Utenti - Ruolo"

Nell'elenco vengono visualizzati tutti gli utenti aggiunti con il relativo ruolo assegnato. Quando si aggiunge un utente, il programma assegna di default il ruolo **Bambino**. Facendo clic con il mouse sul ruolo visualizzato, è possibile passare a un altro ruolo.

> **Nota**
> Non è possibile eliminare l'utente *Standard*.

Ruoli

Campo

Immettere nel campo il nome del ruolo che si desidera aggiungere ai ruoli utente.

Modifica

Il pulsante "**Modifica**" consente di configurare il ruolo selezionato. Viene visualizzata una finestra di dialogo nella quale è possibile definire URL consentiti e non consentiti per il ruolo, nonché contenuti Web non consentiti in base alle categorie. Vedere Proprietà del ruolo.

Aggiungi

Il pulsante consente di aggiungere all'elenco dei ruoli disponibili il ruolo immesso nel campo.

Elimina

Il pulsante consente di eliminare dall'elenco il ruolo selezionato.

Elenco

Nell'elenco vengono visualizzati tutti i ruoli immessi. Facendo doppio clic su un ruolo, si apre la finestra di dialogo per la definizione del ruolo.

> **Nota**
> Non è possibile eliminare i ruoli già assegnati a un utente.

Argomenti correlati:

- Informazioni su Safe Browsing
- Proprietà del ruolo
- Durata utilizzo
- Intervallo di tempo dell'utilizzo

10.8.1 Proprietà del ruolo

Nella finestra **Proprietà del ruolo** è possibile definire un ruolo selezionato per l'utilizzo di Internet.

È possibile consentire o non consentire esplicitamente l'accesso agli URL. È possibile bloccare i contenuti Web in base alla selezione di determinate categorie. È possibile limitare temporalmente l'utilizzo di Internet.

Controlla l'accesso ai seguenti URL

Nell'elenco vengono visualizzati tutti gli URL immessi con le regole assegnate *Blocca* o *Consenti*. Quando si aggiunge un URL, viene assegnata di default la regola *Blocca*. Facendo clic sulla regola è possibile cambiare la regola assegnata.

Aggiungi URL

Immettere nel campo gli URL che devono essere controllati dalla funzione di protezione bambini. È possibile inserire parti di URL definendo il livello del dominio con punti iniziali o finali: **.domainname.it** per tutte le pagine e tutti i domini secondari del dominio. Per indicare una pagina Web con un dominio di livello superiore a piacere (.com o .net), utilizzare un punto finale: domainname. Se si utilizza una sequenza di caratteri senza punto iniziale o finale, viene interpretata come dominio di livello superiore, ad es. **net** per tutti i domini NET (www.domain.net). È possibile utilizzare anche la wildcard ***** per un numero di caratteri a piacere. Per definire il livello del dominio, utilizzare anche punti iniziali o finali in combinazione con wildcard.

> **Nota**
> Alle regole URL viene data la priorità in base al numero delle parti di nome immesse (label) del dominio. Tante più parti di nome si immettono per il dominio, tanto maggiore sarà la priorità della regola. Es.:
> URL: www.avira.com - Regola: Consenti
> URL: .avira.com - Regola: Blocca
> Il set di regole consente tutti gli URL del dominio www.avira.com. L'URL "forum.avira.com" viene bloccato.

> **Nota**
> Immettendo . oppure * vengono compresi tutti gli URL. Utilizzare tali caratteri se

si desidera consentire, ad esempio per il ruolo *Bambino*, solo pochi siti Web indicati in modo esplicito, ad es. nel seguente set di regole:
URL: ***** o **.** - Regola: Blocca
URL: kids.yahoo.com - Regola: Consenti
URL: kids.nationalgeographic.com - Regola: Consenti
Il set di regole blocca tutti gli URL tranne gli URL con i domini "kids.yahoo.com" e "kids.nationalgeographic.com".

Aggiungi

Il pulsante consente di aggiungere all'elenco degli URL controllati l'URL immesso.

Elimina

Il pulsante consente di eliminare dall'elenco degli URL controllati l'URL selezionato.

Blocca l'accesso agli URL appartenenti alle seguenti categorie

Se l'opzione è attivata, vengono bloccati i contenuti Web appartenenti alle categorie selezionate del relativo elenco.

Durata utilizzo consentita

Con il pulsante **Durata utilizzo consentita** si apre una finestra di dialogo in cui è possibile impostare una limitazione temporale all'utilizzo di Internet per il ruolo che si sta configurando. È possibile stabilire l'utilizzo di Internet mensile, settimanale, oppure differenziato a seconda che si tratti di giorni infrasettimanali o del weekend. Nella finestra di dialogo successiva è possibile stabilire gli intervalli di tempo precisi per ogni giorno della settimana. Vedere Durata utilizzo.

Esempio: URL da controllare

- `www.avira.com` -OPPURE- `www.avira.com/*`
  = comprende tutti gli URL con il dominio `www.avira.com`:
  www.avira.com/en/pages/index.php, *www.avira.com/en/support/index.html*, *www.avira.com/en/download/index.html*,...
  Non sono compresi URL con il dominio www.avira.com/it.
- `avira.com` -OPPURE- `*.avira.com`
  = comprende tutti gli URL con dominio di livello secondario o superiore `avira.com`. Tali dati comprendono tutti i domini secondari esistenti di `.avira.com`:
  www.avira.com, *forum.avira.com*,...
- `avira.` -OPPURE- `*.avira.*`
  = comprende tutti gli URL con dominio di livello secondario `avira`. Tali dati comprendono tutti i domini esistenti di livello superiore o i domini secondari di `.avira.`: *www.avira.com, www.avira.de, forum.avira.com*,...
- `.*domain*.*`
  Comprende tutti gli URL che contengono un dominio di livello secondario con la sequenza di caratteri "`domain`": *www.domain.com*, *www.new-domain.it*, *www.sample-domain1.it*, ...

- `net` -OPPURE- `*.net`
  = comprende tutti gli URL con dominio di livello superiore "`net`": *www.name1.net*, *www.name2.net*,...

Argomenti correlati:

- Informazioni su Safe Browsing
- Configurazione di Safe Browsing
- Durata utilizzo
- Intervallo di tempo dell'utilizzo

10.8.2 Durata utilizzo

Nella finestra **Durata utilizzo** è possibile definire una durata massima dell'utilizzo di Internet per un ruolo utente. L'utilizzo temporale di Internet viene stabilito sulla base di richieste di collegamento a Internet che avvengono con un intervallo minimo di 5 minuti. Per ogni ruolo può essere indicato il tempo di navigazione massimo desiderato settimanale, mensile, oppure differenziato a seconda che si tratti di giorni infrasettimanali o del weekend.

Limita temporalmente utilizzo Internet

Questa opzione consente di limitare la durata dell'utilizzo di Internet per tutti gli utenti a cui è assegnato il ruolo. In caso di superamento della durata di utilizzo consentita, le pagine Web richieste, ovvero richiamate, dall'utente vengono bloccate. Nel browser Web compare un avviso.

Limitazione temporale per settimana, mese, giorno (lu-ve, sa-do)

È possibile indicare la durata di utilizzo desiderata mediante il cursore di scorrimento o i tasti freccia a destra del campo. Inoltre, la durata di utilizzo può essere impostata direttamente nei campi temporali. A tal fine si osservi il formato indicato per l'indicazione temporale.

Le indicazioni diverse per la durata di utilizzo non vengono uniformate dal programma. Il programma utilizza ogni volta il valore adatto più basso per limitare la durata di utilizzo.

Intervallo di tempo preciso

Con il pulsante **Intervallo di tempo preciso** si apre una finestra di dialogo in cui è possibile stabilire gli orari giornalieri per la durata di utilizzo massima definita. Vedere Intervallo di tempo dell'utilizzo.

Argomenti correlati:

- Informazioni su Safe Browsing
- Configurazione di Safe Browsing
- Proprietà del ruolo
- Intervallo di tempo dell'utilizzo

10.8.3 Intervallo di tempo dell'utilizzo

Nella finestra **Intervallo di tempo dell'utilizzo** è possibile definire i tempi di utilizzo consentiti per la durata massima dell'utilizzo di Internet indicata per un ruolo: è possibile stabilire determinati orari per l'utilizzo di Internet per ogni giorno della settimana.

Consenti utilizzo di Internet solo agli orari indicati

Questa opzione consente di stabilire gli orari di navigazione per tutti gli utenti a cui è assegnato il ruolo configurato. Se gli utenti del computer utilizzano Internet al di fuori degli orari consentiti, le pagine Web richiamate vengono bloccate. Nel browser Web compare un messaggio.

- Per stabilire gli orari dell'utilizzo di Internet, contrassegnare gli intervalli di tempo desiderati.

  Vi sono le seguenti possibilità di contrassegnare gli orari autorizzati o bloccati:

  - **Per stabilire gli orari dell'utilizzo di Internet:** fare clic sui campi temporali non contrassegnati desiderati o trascinare il cursore sui campi temporali non contrassegnati utilizzando il tasto sinistro del mouse.
  - **Per bloccare gli orari dell'utilizzo di Internet:** fare clic sui campi temporali contrassegnati desiderati o trascinare il cursore sui campi temporali contrassegnati utilizzando il tasto sinistro del mouse.

- Fare clic con il tasto destro del mouse sui campi temporali del giorno desiderato per richiamare in una finestra di dialogo gli intervalli di tempo indicati. Esempio *Utilizzo di Internet bloccato dalle 00:00 alle 11:00.*

Argomenti correlati:

- Informazioni su Safe Browsing
- Configurazione di Safe Browsing
- Proprietà del ruolo
- Durata utilizzo

10.9 Generale

10.9.1 Categorie di minacce

Selezione delle categorie estese delle minacce

Il prodotto Avira protegge dai virus del computer. Inoltre, si ha la possibilità di effettuare una scansione differenziata in base alle seguenti categorie di minacce.

- Adware
- Adware/Spyware
- Applicazioni

- Software di controllo backdoor
- File con estensioni nascoste
- Programmi di selezione a pagamento
- Phishing
- Programmi che violano la privacy dell'utente
- Programmi ludici
- Giochi
- Software ingannevole
- Programmi zip runtime insoliti

Facendo clic sulla casella appropriata viene attivata (spuntata) o disattivata (non spuntata) la modalità selezionata.

Attiva tutti

Se l'opzione è attivata vengono attivate tutte le modalità.

Valori standard

Questo pulsante ripristina i valori standard predefiniti.

> **Nota**
> Se viene disattivata una modalità, i file riconosciuti come tale tipo di programma non verranno più segnalati. Non viene riportata alcuna segnalazione nemmeno sul file di report.

10.9.2 Protezione avanzata

Protezione avanzata

ProActiv

Attivazione di ProActiv

Se l'opzione è attivata, i programmi presenti sul computer vengono monitorati alla ricerca di azioni sospette. Se viene rilevato un comportamento tipico del malware, si riceve un messaggio. È possibile bloccare il programma oppure proseguire con la sua esecuzione selezionando "**Ignora**". Dal monitoraggio sono esclusi: i programmi classificati come affidabili, i programmi affidabili e con firma che sono contenuti di default nel filtro delle applicazioni consentite, tutti i programmi che sono stati aggiunti dall'utente al filtro delle applicazioni dei programmi consentiti.

L'impiego di ProActiv consente di proteggere il computer da minacce nuove e sconosciute per le quali non esistono ancora definizioni di virus né euristiche. La tecnologia ProActiv è integrata nel componente Real-Time Protection e consente di osservare e analizzare le

azioni dei programmi. Nel comportamento dei programmi vengono ricercati modelli di azioni tipici dei programmi di malware: tipi di azione e relativa sequenza. Se un programma presenta un comportamento tipico dei programmi di malware, il sistema gestisce il problema come un rilevamento di virus e invia una segnalazione: l'utente può bloccare l'esecuzione del programma o ignorare la segnalazione e continuare. È possibile classificare il programma come affidabile e aggiungerlo così al filtro delle applicazioni dei programmi consentiti. È possibile inoltre aggiungere il programma al filtro delle applicazioni dei programmi da bloccare indicando **Blocca sempre**.

Per rilevare i comportamenti sospetti, il componente ProActiv utilizza set di regole che sono state sviluppate da Avira Malware Research Center. Tali set di regole sono alimentati dalle banche dati di Avira. Per la raccolta delle informazioni nelle banche dati di Avira, ProActiv invia informazioni relative a programmi sospetti notificati. Durante l'installazione di Avira è possibile disattivare l'inoltro dei dati alle banche dati di Avira.

> **Nota**
> La tecnologia ProActiv non è ancora disponibile per i sistemi a 64 bit!

Protection Cloud

Attiva Protection Cloud

Le identificazioni digitali di tutti i file sospetti vengono trasmesse ad Avira Cloud per il rilevamento online dinamico. I file delle applicazioni vengono visualizzati immediatamente come puliti, infetti o sconosciuti.

Il sistema Protection Cloud funge da nodo centrale per il rilevamento di attacchi cibernetici contro la Community di Avira. I file a cui il PC in uso accede vengono confrontati con i modelli di file memorizzati nel sistema cloud. Dal momento che la maggior parte del lavoro si svolge sul cloud, il programma di protezione locale richiede meno risorse.

Durante ogni **scansione rapida del sistema**, viene creato un elenco dei percorsi dei file che i programmi di malware utilizzano come destinazione. Nell'elenco sono contenuti, ad esempio, i processi in corso, le utility e i programmi di esecuzione automatica in uso. Da ogni file viene creata una somma di controllo digitale ("identificazione digitale"), che viene successivamente inviata al sistema Protection Cloud e classificata come "Clean" o "Malware". I file di programma sconosciuti saranno caricati per l'analisi del sistema Protection Cloud.

Conferma manuale in caso di invio di file sospetti ad Avira

È possibile controllare l'elenco dei file sospetti da caricare in Protection Cloud e scegliere manualmente i file che si desidera caricare.

Scansione file in tempo reale

Se questa opzione è attivata, i file sconosciuti vengono inviati a Protection Cloud per l'analisi non appena vengono aperti.

Mostra stato per il caricamento dei file su Avira Protection Cloud

All'interno di una finestra, le seguenti informazioni relative ai file caricati vengono visualizzate sotto forma di barra di avanzamento:

- percorso file

- nome file

- stato (caricamento/analisi in corso)

- risultato (pulito/infetto)

In *Applicazioni da bloccare* è possibile inserire applicazioni classificate come dannose che si desidera vengano bloccate di default da ProActiv di Avira. Le applicazioni inserite non possono essere eseguite sul computer. Con l'opzione **Blocca sempre questo programma**, è possibile aggiungere programmi al filtro delle applicazioni da bloccare anche attraverso le comunicazioni di Real-Time Protection relative a un comportamento sospetto da parte di un programma.

Applicazioni da bloccare

Applicazione

Nell'elenco sono riportate tutte le applicazioni classificate come dannose e aggiunte dall'utente durante la configurazione o derivanti dai messaggi del componente ProActiv. Tali applicazioni vengono bloccate da ProActiv di Avira e non possono essere eseguite sul sistema. Ogni volta che viene avviato un programma da bloccare, viene visualizzato un messaggio del sistema operativo. Le applicazioni da bloccare vengono identificate da ProActiv di Avira in base al percorso indicato e al nome del file e bloccate indipendentemente dal contenuto.

Campo

Immettere in questo campo l'applicazione da bloccare. Per identificare l'applicazione, è necessario inserire il percorso completo e il nome del file con la relativa estensione. Il percorso indicato deve contenere il drive in cui si trova l'applicazione oppure iniziare con una variabile d'ambiente.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare l'applicazione da bloccare.

Aggiungi

Con il pulsante "**Aggiungi**" è possibile aggiungere l'applicazione indicata nel campo all'elenco delle applicazioni da bloccare.

> **Nota**
> Non è possibile aggiungere le applicazioni necessarie al funzionamento del sistema operativo.

Elimina

Con il pulsante "**Elimina**" è possibile rimuovere un'applicazione selezionata dall'elenco delle applicazioni da bloccare.

In *Applicazioni da escludere* sono elencate le applicazioni escluse dal monitoraggio del componente ProActiv: i programmi firmati che sono classificati come affidabili e sono contenuti di default nell'elenco, tutte le applicazioni classificate come affidabili dall'utente e inserite nel filtro delle applicazioni: nella configurazione è possibile aggiungere delle applicazioni all'elenco delle applicazioni consentite. È inoltre possibile aggiungere delle applicazioni segnalate nelle comunicazioni di Real-Time Protection relative a un comportamento sospetto da parte di un programma attivando nei messaggi di Real-Time Protection l'opzione **Programma attendibile**.

Applicazioni da escludere

Applicazione

L'elenco contiene le applicazioni escluse dal monitoraggio del componente ProActiv. Nelle impostazioni di default dopo l'installazione, l'elenco contiene applicazioni firmate di produttori attendibili. È possibile inserire applicazioni classificate come attendibili mediante la configurazione o i messaggi di Real-Time Protection. Il componente ProActiv identifica le applicazioni in base al percorso, al nome del file e al contenuto. La verifica dei contenuti è utile poiché a un programma possono essere aggiunti codici dannosi in un secondo momento, in seguito a modifiche come gli aggiornamenti. Specificando la **modalità**, è possibile stabilire se deve essere eseguita una verifica del contenuto: con la modalità "*Contenuto*" vengono verificate le modifiche del contenuto nei file delle applicazioni indicate con percorso e nome prima che vengano escluse dal monitoraggio mediante il componente ProActiv. Nel caso di una modifica del contenuto del file, l'applicazione viene nuovamente monitorata dal componente ProActiv. Con la modalità "*Percorso*" non avviene alcuna verifica del contenuto prima che l'applicazione venga esclusa dal monitoraggio mediante Real-Time Protection. Per cambiare la modalità di esclusione, fare clic sulla modalità indicata.

Attenzione
Utilizzare la modalità *Percorso* solo in casi eccezionali. In seguito a un aggiornamento, è possibile che a un'applicazione vengano aggiunti codici dannosi. L'applicazione che originariamente era innocua diventa un programma malware.

Nota
Alcune applicazioni affidabili, ad esempio tutti i componenti applicativi del prodotto Avira, sono esclusi di default dal monitoraggio mediante ProActiv, tuttavia non sono riportati nell'elenco.

Campo

Inserire in questo campo l'applicazione che si intende escludere dal monitoraggio mediante il componente ProActiv. Per identificare l'applicazione, è necessario inserire il percorso completo e il nome del file con la relativa estensione. Il percorso indicato deve contenere il drive in cui si trova l'applicazione oppure iniziare con una variabile d'ambiente.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare l'applicazione da escludere.

Aggiungi

Con il pulsante "**Aggiungi**" è possibile accettare l'applicazione indicata nel campo nell'elenco delle applicazioni da escludere.

Elimina

Con il pulsante "**Elimina**" è possibile rimuovere un'applicazione selezionata dall'elenco delle applicazioni da escludere.

10.9.3 Password

Tutti i prodotti Avira possono essere protetti in diverse sezioni mediante una password. Se si inserisce una password questa verrà richiesta ogni volta che si desidera aprire una sezione protetta.

Password

Inserimento password

Inserire qui la password desiderata. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*). È possibile inserire un numero massimo di 20 caratteri. Se è stata inserita una password, il programma negherà l'accesso in caso di inserimento di password errata. Un campo vuoto equivale a "Nessuna password".

Conferma

Inserire nuovamente la password per conferma. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*).

> **Nota**
> Attenzione alle lettere maiuscole o minuscole!

Aree protette da password

Il prodotto Avira consente di proteggere con password ogni singola sezione. Facendo clic sulla casella appropriata, la richiesta di password per alcune sezioni può essere disattivata o riattivata.

Sezione protetta da password	Funzione
Control Center	Se l'opzione è attivata, per l'avvio del Control Center è necessaria la password impostata.
Attiva/disattiva Real-Time Protection	Se l'opzione è attivata, per l'attivazione e la disattivazione di Real-Time Protection di Avira è necessario inserire la password impostata.
Attiva/disattiva Mail Protection	Se l'opzione è attivata, per l'attivazione e la disattivazione di Mail Protection è necessario inserire la password impostata.
Attiva/disattiva Web Protection	Se l'opzione è attivata, per l'attivazione e la disattivazione di Web Protection è necessario inserire la password impostata.
Attiva/disattiva Safe Browsing	Se l'opzione è attivata, per l'attivazione e la disattivazione della Protezione dei bambini è necessario inserire la password impostata.
Quarantena	Se l'opzione è attivata, per l'attivazione e la disattivazione di tutte le sezioni di Gestore della quarantena è necessario inserire la password impostata. Facendo clic sulla casella appropriata, la richiesta di password per alcune sezioni può essere disattivata o riattivata.
Ripristina gli oggetti infetti	Se l'opzione è attivata, per il ripristino degli oggetti è necessario inserire la password impostata.
Nuovo controllo di oggetti infetti	Se l'opzione è attivata, per il nuovo controllo degli oggetti è necessario inserire la password impostata.

Apri gli oggetti infetti	Se l'opzione è attivata, per la visualizzazione delle proprietà degli oggetti è necessario inserire la password impostata.
Elimina gli oggetti infetti	Se l'opzione è attivata, per l'eliminazione degli oggetti è necessario inserire la password impostata.
Invia e-mail ad Avira	Se l'opzione è attivata, per l'invio degli oggetti al Malware Research Center Avira è necessario inserire la password impostata.
Copia di oggetti infetti	Se l'opzione è attivata, per copiare gli oggetti infetti è necessario inserire la password impostata.
Aggiungi e modifica job	Se l'opzione è attivata, per aggiungere e modificare job nel Pianificatore è necessario inserire la password impostata.
Configurazione	Se l'opzione è attivata, è possibile configurare il programma solo dopo l'inserimento della password impostata.
Installazione/Disinstallazione	Se l'opzione è attivata, per installare o disinstallare il programma è necessaria la password impostata.

10.9.4 Sicurezza

Esecuzione automatica

Blocca esecuzione automatica

Se l'opzione è attivata, la funzione di esecuzione automatica di Windows viene bloccata su tutti i drive collegati, come penne USB, CD e DVD, drive di rete. Con la funzione di esecuzione automatica di Windows, i file sui supporti informatici o sui drive di rete vengono letti immediatamente al momento dell'inserimento o del collegamento; in questo modo i file possono essere avviati e riprodotti automaticamente. Tuttavia questa funzionalità nasconde un rischio per la sicurezza molto elevato, poiché con l'avvio automatico dei file è possibile che vengano installati malware e programmi indesiderati. La funzione di esecuzione automatica è particolarmente critica nel caso delle penne USB poiché su questi supporti i file possono modificarsi continuamente.

Escludi CD e DVD

Se l'opzione è attivata, la funzione di esecuzione automatica è consentita su CD e DVD.

> **Attenzione**
> Disattivare la funzione di esecuzione automatica per CD e DVD solo se si è sicuri che si tratti di supporti informatici assolutamente affidabili.

Protezione del sistema

Proteggi il file host di Windows da modifiche

Se l'opzione è attivata, il file host di Windows è disponibile in sola lettura. Non è più possibile manipolare il file. Il malware non è più, ad esempio, in grado di deviare l'utente su pagine Internet indesiderate. Questa opzione è attivata di default.

Tutela del prodotto

> **Nota**
> Se durante l'installazione personalizzata si è deciso di non installare Real-Time Protection, le opzioni di tutela del prodotto non saranno disponibili.

Proteggi i processi da una chiusura indesiderata

Se l'opzione è attivata, tutti i processi del programma vengono protetti da chiusura indesiderata dovuta a virus e malware o da chiusura involontaria di un utente, ad esempio mediante Task Manager. Questa opzione è attivata di default.

Protezione del processo avanzata

Se l'opzione è attivata, tutti i processi del programma vengono protetti da chiusura indesiderata con metodi avanzati. La protezione avanzata del processo consuma molte più risorse rispetto alla protezione di processo base. L'opzione è attivata di default. Per disattivare l'opzione è necessario riavviare il computer.

> **Nota**
> La protezione del processo in Windows XP a 64 bit non è disponibile.

> **Attenzione**
> Se la protezione del processo è attivata, possono verificarsi problemi di interazione con altri software. In tal caso disattivare la protezione del processo.

Proteggi i file e le voci di registrazione dalla manipolazione

Se l'opzione è attivata, tutte le voci di registro del programma e tutti i dati del programma (file binari e di configurazione) vengono protetti da manipolazione. La protezione da manipolazione comprende la protezione da interventi di scrittura, eliminazione e talvolta di lettura sulle voci del registro o sui file di programma da parte di utenti o di programmi estranei. Per attivare l'opzione è necessario riavviare il computer.

Attenzione
Tenere presente che, se l'opzione è disattivata, è possibile che la riparazione di computer infetti a causa di determinati tipi di malware non possa essere effettuata.

Nota
Se l'opzione è attivata, è possibile apportare modifiche alla configurazione oppure a job di scansione e aggiornamento solo tramite l'interfaccia utente.

Nota
La protezione dei file e delle voci di registrazione in Windows XP a 64 bit non è disponibile.

10.9.5 WMI

Assistenza per Windows Management Instrumentation (WMI)

Windows Management Instrumentation è una tecnologia di gestione fondamentale di Windows che consente, mediante linguaggi di script e di programmazione in lettura e in scrittura, di accedere in locale e in remoto alle impostazioni dei computer Windows. Il prodotto Avira supporta WMI e rende disponibili dati (informazioni di stato, dati statistici, report, job pianificati ecc.), eventi in un'interfaccia. Tramite WMI è possibile richiamare dati operativi del programma.

Attiva assistenza WMI

Se l'opzione è attivata, è possibile richiamare i dati operativi del programma tramite WMI.

10.9.6 Eventi

Limitare l'estensione della banca dati degli eventi

Limita l'estensione ad un massimo di n immissioni

Se l'opzione è attiva, il numero massimo delle immissioni nella banca dati degli eventi è limitato a un preciso numero; i valori consentiti sono: da 100 a 10.000 immissioni. Se il numero delle immissioni viene superato, gli inserimenti più vecchi vengono eliminati.

Elimina tutti gli eventi più vecchi di n giorno/i

Se l'opzione è attiva, dopo un numero determinato di giorni gli eventi vengono eliminati dalla banca dati degli eventi; i valori consentiti sono: da 1 a 90 giorni. Di default questa opzione è attivata con un valore di 30 giorni.

Nessun limite

Se l'opzione è attivata, le dimensioni della banca dati degli eventi non sono limitate. Sull'interfaccia del programma, alla voce Eventi, viene però visualizzato un massimo di 20.000 immissioni.

10.9.7 Report

Limita i report

Limita il numero a un massimo di n pezzi

Se l'opzione è attiva, il numero massimo di report può essere limitato a un determinato numero; i valori consentiti sono: da 1 a 300. Se il numero indicato viene superato, i report più vecchi vengono eliminati.

Elimina tutti i report più vecchi di n giorni

Se l'opzione è attiva, i report vengono automaticamente eliminati dopo un determinato numero di giorni; i valori consentiti sono: da 1 a 90 giorni. Di default questa opzione è attivata con un valore di 30 giorni.

Nessun limite

Se l'opzione è attiva il numero di report non è limitato.

10.9.8 Directory

Percorso temporaneo

Utilizza le impostazioni predefinite

Se l'opzione è attivata vengono utilizzate le impostazioni del sistema per la gestione dei file temporanei.

> **Nota**
> Per sapere dove vengono salvati i file temporanei, ad esempio in Windows XP, accedere a: **Start > Impostazioni > Pannello di controllo > Sistema >** scheda

> "**Avanzate**" > pulsante "**Variabili d'ambiente**". Le variabili temporanee (`TEMP`, `TMP`) per l'utente di volta in volta registrato e per le variabili di sistema (`TEMP`, `TMP`) sono visibili qui con i loro rispettivi valori.

Utilizza la seguente directory

Se l'opzione è attivata viene utilizzato il percorso visualizzato nel campo.

Campo

In questo campo è possibile immettere il percorso in cui si desidera che vengano salvati i file temporanei del programma.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il percorso temporaneo desiderato.

Standard

Il pulsante crea la directory predefinita per il percorso temporaneo.

10.9.9 Avviso acustico

In caso di rilevamento di un virus o di malware tramite Scanner o Real-Time Protection, viene emesso un avviso acustico in modalità di azione interattiva. È possibile attivare o disattivare l'avviso acustico nonché selezionare un file WAVE alternativo come avviso acustico.

> **Nota**
> La modalità di azione di Scanner viene impostata nella configurazione in Sicurezza del computer > Scanner > Scansione > Azione in caso di rilevamento. La modalità di azione di Real-Time Protection viene impostata nella configurazione in Sicurezza del computer > Real-Time Protection > Scansione > Azione in caso di rilevamento.

Nessun avviso

Se l'opzione è attivata, non viene emesso alcun avviso acustico in caso di rilevamento di un virus tramite Scanner o Real-Time Protection.

Emetti tramite casse PC (solo in modalità interattiva)

Se l'opzione è attivata, viene emesso un avviso acustico con suono standard in caso di rilevamento di un virus tramite Scanner o Real-Time Protection. L'avviso acustico viene emesso tramite l'altoparlante interno del PC.

Utilizza il seguente file WAVE (solo in modalità interattiva)

Se l'opzione è attivata, in caso di rilevamento di un virus tramite Scanner o Real-Time Protection, viene emesso un avviso acustico con il file WAVE selezionato. Il file WAVE selezionato viene riprodotto tramite un altoparlante collegato esternamente.

File WAVE

In questo campo è possibile inserire il nome e il percorso corrispondente di un file audio a scelta. L'avviso acustico standard del programma è registrato come impostazione predefinita.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file desiderato tramite Esplora file.

Test

Questo pulsante serve a testare il file WAVE selezionato.

10.9.10 Avvisi

In caso di determinati eventi, il prodotto Avira genera notifiche sul desktop, i cosiddetti messaggi a tendina, per informare l'utente di eventuali pericoli o della riuscita o meno dell'esecuzione di un dato programma come, per esempio, un aggiornamento. È possibile attivare o disattivare in **Avvisi** la funzione di notifica per specifici eventi.

Nel caso delle notifiche sul desktop è possibile disattivare direttamente le notifiche sul messaggio a tendina. È possibile annullare la disattivazione della notifica nella finestra di configurazione **Avvisi**.

Aggiornamento

Avviso se l'aggiornamento risale a più di n giorni fa

In questo campo è possibile inserire il numero massimo di giorni che possono trascorrere dall'ultimo aggiornamento. Superato questo intervallo di tempo, il Control Center visualizzerà sotto Stato un'icona rossa per lo stato dell'aggiornamento.

Avvisa se il file VDF non è aggiornato

Se l'opzione è attivata, si riceve un avviso in caso di file di definizione dei virus non aggiornato. Grazie all'opzione "Avviso se l'aggiornamento risale a più di n giorni fa", è possibile configurare un intervallo temporale.

Avvisi/indicazione nelle seguenti situazioni

Utilizzo di una connessione dial-up

Se l'opzione è attivata, l'utente è avvisato con una notifica sul desktop quando un programma di selezione stabilisce una connessione sul computer tramite la rete telefonica o ISDN. In caso di programmi di selezione esiste il rischio che si tratti di un

dialer sconosciuto e indesiderato, che stabilisce una connessione a pagamento. Vedere Categorie di minacce: Programmi di selezione a pagamento.

File aggiornati correttamente

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando è stato completato con successo un aggiornamento e sono stati aggiornati file.

Aggiornamento non riuscito

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando l'aggiornamento non riesce, il che significa che non è stato possibile stabilire una connessione con il server di download oppure non è stato possibile installare i file di aggiornamento.

Non sono necessari aggiornamenti

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando viene lanciato un aggiornamento ma non è necessario installare alcun file perché il programma è già aggiornato.

11. Icona della barra delle applicazioni

L'icona della barra delle applicazioni mostra lo stato di Real-Time Protection.

Icona	Descrizione
	Avira Real-Time Protection è attivo
	Avira Real-Time Protection non è attivo

Voci del menu contestuale

- **Attiva Real-Time Protection**: attiva o disattiva Avira Real-Time Protection.
- **Attiva Mail Protection**: attiva o disattiva Avira Mail Protection.
- **Attiva Web Protection**: attiva o disattiva Avira Web Protection.
  - **Attiva Windows Firewall**: attiva o disattiva Windows Firewall (questa funzione sarà disponibile a partire da Windows 8).
- **Avvia Avira Ultimate Protection Suite**: apre Control Center.
- **Configura Avira Ultimate Protection Suite** : apre la configurazione.
- **I miei messaggi**: apre una finestra con i messaggi più recenti relativi al prodotto Avira.
- **Le mie impostazioni di comunicazione**: apre il Centro Abo per le comunicazioni del prodotto
- **Avvia l'aggiornamento**: avvia un aggiornamento.
- **Guida in linea**: apre la guida in linea.
- **Informazioni su Avira Ultimate Protection Suite**:
  apre una finestra di dialogo con informazioni sul prodotto Avira: prodotto, versione e licenza.
- **Avira su Internet**:
  apre il portale Web di Avira su Internet. Il prerequisito essenziale è l'accesso attivo a Internet.

12. Notifiche sul prodotto

12.1.1 Centro abbonamenti avvisi sui prodotti

Facendo clic su **Le mie impostazioni di comunicazione** nel menu contestuale dell'icona Tray di Avira oppure facendo clic sull'icona della **Configurazione** nella finestra **I miei messaggi** viene visualizzato il *Centro abbonamenti avvisi sui prodotti* sul nostro sito Web.

- È possibile controllare il flusso di informazioni delle comunicazioni sul prodotto facendo clic sul pulsante **ATTIVA/DISATTIVA**.
- Fare clic su **Aggiorna profilo** per memorizzare il proprio profilo personale di comunicazione.
  - ↳ Verrà visualizzato un messaggio indicante che il profilo di comunicazione è stato aggiornato.

Per mettersi in contatto con Avira online, fare clic su uno dei link.

12.1.2 Messaggi attuali

La finestra *I miei messaggi* funge da interfaccia per la comunicazione. Essa vi informa sugli sviluppi attuali della sicurezza in Internet, sulle novità dei prodotti Avira (aggiornamenti, upgrade e informazioni sulla licenza) e sui virus.

Se non è presente nessun messaggio, viene visualizzato il messaggio *Non ci sono nuovi messaggi*. Fare clic su **OK** per chiudere la finestra.

In presenza di nuovi messaggi sono disponibili le seguenti possibilità:

- Fare clic su **Ricorda più tardi** per leggere i messaggi in un altro momento.
- Fare clic sul segno più **+** per leggere i dettagli del messaggio.
  - ↳ A seconda del tipo di messaggio verrà aperto il sito Web di Avira oppure verrà visualizzata una nuova finestra informativa.
- Fare clic sul segno **x** per chiudere i messaggi uno ad uno.
- Fare clic sull'icona della **Configurazione** nella testata della finestra per memorizzare il proprio profilo di comunicazione personale.

13. FireWall

Avira Ultimate Protection Suite permette di monitorare e regolare il traffico dati in entrata e in uscita in base alle impostazioni del computer:

- Windows Firewall

A partire da Windows 7 Avira FireWall non è più contenuto in Avira Ultimate Protection Suite. È tuttavia possibile controllare Windows Firewall tramite i centri di configurazione e controllo.

13.1 Windows Firewall

A partire da Windows 7 Avira FireWall non è più contenuto in Avira Ultimate Protection Suite. È comunque possibile controllare Windows Firewall tramite il centro di configurazione e controllo. Sono quindi disponibili le seguenti possibilità di impostazione di Windows Firewall:

Attivare Windows Firewall in Control Center

È possibile attivare o disattivare Windows Firewall facendo clic sul pulsante **ATTIVO/NON ATTIVO** dell'opzione *FireWall* in **Stato > Sicurezza Internet**.

Monitorare lo stato di Windows Firewall in Control Center

È possibile monitorare lo stato di Windows Firewall nella rubrica **SICUREZZA INTERNET > FireWall** e ripristinare le impostazioni consigliate facendo clic sul pulsante **Risoluzione del problema**.

14. Aggiornamenti

14.1 Aggiornamenti

L'efficacia di un software antivirus dipende dall'aggiornamento del programma, in particolare del file di definizione dei virus e del motore di ricerca. Per l'esecuzione degli aggiornamenti, il componente Updater è integrato nel prodotto Avira. Updater garantisce che il prodotto Avira sia sempre il più aggiornato possibile e che sia in grado di rilevare i nuovi virus che compaiono quotidianamente. Updater aggiorna i seguenti componenti:

- File di definizione dei virus:

  Il file di definizione dei virus contiene il modello di rilevamento del programma dannoso che il prodotto Avira utilizza nella scansione per virus e malware nonché nella riparazione di oggetti infetti.

- Motore di ricerca:

  Il motore di ricerca contiene i metodi che vengono utilizzati dal prodotto Avira per la scansione per virus e malware.

- File di programma (aggiornamento del prodotto):

  I pacchetti di aggiornamento del prodotto mettono a disposizione ulteriori funzioni per i singoli componenti del programma.

Durante un aggiornamento viene verificato lo stato di aggiornamento del file di definizione dei virus, dei file di programma e del motore di ricerca e, se necessario, tali componenti vengono aggiornati. Terminato un aggiornamento del prodotto può essere necessario riavviare il sistema. Se l'aggiornamento avviene solo per il file di definizione dei virus e per il motore di ricerca, non è necessario riavviare il computer.

Se dovesse essere necessario un riavvio dopo un aggiornamento del prodotto, è possibile decidere se proseguire con l'aggiornamento o se si preferisce ricevere un promemoria successivamente. Se si decide di proseguire con l'aggiornamento, è tuttavia possibile stabilire quando debba avvenire il riavvio.

Se si decide di effettuare l'aggiornamento in un momento successivo, vengono comunque aggiornati il file delle definizioni antivirus e il motore di ricerca, ma non i file di programma.

> **Nota**
> L'aggiornamento del prodotto non si completa fino a quando non è stato effettuato il riavvio.
>
> **Nota**
> Per motivi di sicurezza, Updater verifica se il file host di Windows del computer è stato modificato, ad esempio con manipolazione da parte di malware dell'URL di aggiornamento a seguito della quale Updater viene indirizzato a pagine di

download indesiderate. Se il file host di Windows è stato manipolato, l'evento viene riportato nel file di record di Updater.

Viene automaticamente eseguito un aggiornamento con il seguente intervallo: 2 ore.

In Control Center in **Pianificatore** è possibile configurare ulteriori job di aggiornamento che Updater deve eseguire a intervalli definiti. È inoltre possibile avviare l'aggiornamento manualmente:

- In Control Center: nel menu **Aggiornamento** e dalla rubrica **Stato**
- Tramite il menu contestuale dell'icona Tray

Gli aggiornamenti vengono richiamati da Internet tramite un server Web del produttore. Normalmente si utilizza la connessione di rete esistente per collegarsi al server di download di Avira. Questa impostazione standard può essere modificata in Configurazione > Aggiorna.

14.2 Updater

Dopo l'avvio di un aggiornamento si apre la finestra di Updater.

> **Nota**
> Per i job di aggiornamento creati nel Pianificatore è possibile impostare la **modalità di visualizzazione** della finestra di aggiornamento: è possibile scegliere tra le modalità **Invisibile**, **Ridotta** o **Espansa**.

> **Nota**
> Se si lavora con un programma in modalità a schermo intero (ad esempio con i giochi) e l'Updater è in modalità di visualizzazione estesa o ridotta, l'Updater si collega sul desktop. Per evitarlo l'Updater può essere anche lasciato in Modalità di visualizzazione invisibile. In questo modo non si viene informati con la finestra di aggiornamento.

Stato: mostra la procedura corrente dell'Updater.

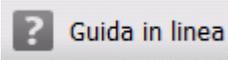
Tempo trascorso: tempo trascorso dall'avvio della procedura di download.

Tempo rimanente: tempo mancante alla conclusione del download.

Velocità: velocità di scaricamento dei file.

Trasferiti: byte già scaricati.

Rimanenti: byte ancora da scaricare.

Pulsanti e link

Pulsante/Link	Descrizione
Guida in linea	Con questo pulsante o link viene aperta questa pagina della guida in linea.
Riduci	La finestra di visualizzazione dell'Updater viene visualizzata ridotta.
Ingrandisci	La finestra di visualizzazione dell'Updater viene ripristinata nelle sue dimensioni originali.
Annulla	La procedura di aggiornamento viene interrotta. L'Updater viene chiuso.

Chiudi	La procedura di aggiornamento è conclusa. La finestra di visualizzazione viene chiusa.
Report	Viene visualizzato il file di report degli aggiornamenti.

15. Risoluzione di problemi, suggerimenti

In questo capitolo vengono riportate informazioni importanti per la risoluzione dei problemi e altri consigli sull'uso del prodotto Avira.

- Vedere il capitolo Assistenza in caso di problemi
- Vedere il capitolo Shortcut
- Vedere il capitolo Centro sicurezza PC di Windows (per Windows XP) o Centro operativo di Windows (a partire da Windows 7)

15.1 Assistenza in caso di problemi

Qui sono reperibili informazioni sulle cause e le soluzioni di eventuali problemi.

- Viene visualizzato il messaggio di errore *Impossibile leggere il file di licenza*.
- Il messaggio di errore *Lo stabilimento della connessione è fallito durante il download del file ...* viene visualizzato nel tentativo di avviare un aggiornamento.
- Impossibile spostare o eliminare virus e malware.
- L'icona Tray mostra uno stato disattivato.
- Il computer diventa estremamente lento se si esegue un backup.
- Il Firewall segnala Avira Real-Time Protection e Avira Mail Protection non appena sono attivi
- Avira Mail Protection non funziona.
- Un'e-mail inviata tramite una connessione TSL è stata bloccata da Mail Protection.
- La chat Web non funziona: i messaggi di chat non vengono visualizzati.

Viene visualizzato il messaggio di errore *Impossibile leggere il file di licenza*.

Causa: il file è protetto.

- Per attivare la licenza non bisogna aprire il file, ma salvarlo nella directory del programma.

Il messaggio di errore *Lo stabilimento della connessione è fallito durante il download del file ...* viene visualizzato nel tentativo di avviare un aggiornamento.

Causa: la connessione Internet non è attiva. Non è pertanto possibile creare un collegamento con il server Web su Internet.

- Provare se altri servizi Internet come WWW o l'e-mail funzionano. Se non funzionano ripristinare la connessione Internet.

Causa: il server proxy non è raggiungibile.

- Verificare se sia cambiato il login per il server proxy e adattare eventualmente la propria configurazione.

Causa: il file *update.exe* non è ammesso dal proprio firewall.

- Assicurarsi che il file *update.exe* sia ammesso dal proprio firewall.

Altrimenti:

- Controllare la configurazione dal percorso Sicurezza del computer > Aggiorna.

Impossibile spostare o eliminare virus e malware.

Causa: il file è stato caricato da Windows ed è attivo.

- Aggiornare il prodotto Avira.
- Se si utilizza il sistema operativo Windows XP, disattivare il ripristino del sistema.
- Avviare il computer in modalità provvisoria.
- Aprire la configurazione del prodotto Avira.
- Selezionare **Scanner > Scansione**, nel campo *File* attivare l'opzione **Tutti i file** e confermare facendo clic su **OK**.
- Avviare una scansione su tutti i drive locali.
- Avviare il computer in modalità normale.
- Eseguire una scansione in modalità normale.
- Se non vengono rilevati altri virus e malware attivare il ripristino del sistema se è disponibile e deve essere utilizzato.

L'icona Tray mostra uno stato disattivato.

Causa: il servizio Real-Time Protection è stato disattivato.

- Fare clic in Control Center sulla voce **Stato** e nel riquadro *Sicurezza del computer* attivare **Real-Time Protection**.

  - OPPURE -

- Fare clic con il tasto destro del mouse sull'icona Tray. Apparirà un menu contestuale. Fare clic su **Attiva Real-Time Protection**.

Causa: Avira Real-Time Protection viene bloccato dal firewall.

- Definire nella configurazione del firewall un permesso generale per Avira Real-Time Protection. Avira Real-Time Protection lavora esclusivamente con l'indirizzo 127.0.0.1 (localhost). Non viene stabilita alcuna connessione Internet. Altrettanto vale per Avira Mail Protection.

Altrimenti:

- Verificare la modalità di attivazione del servizio Avira Real-Time Protection. Eventualmente attivare il servizio: fare clic su **Start > Impostazioni >Pannello di controllo**. Fare doppio clic sulla finestra di configurazione **Servizi** per attivarla (in Windows XP l'applet dei servizi si trova nella sottocartella *Strumenti di amministrazione*). Cercare la voce *Avira Real-Time Protection*. Come modalità di avviamento deve essere inserito `Automatico` e come stato `Avviato`. Avviare il servizio manualmente mediante la selezione della riga corrispondente e del pulsante **Avvia**. Se viene visualizzato un messaggio di errore, verificare la visualizzazione eventi.

Il computer diventa estremamente lento se si esegue un backup.

Causa: Avira Real-Time Protection scansiona tutti i file con i quali lavora il sistema di backup durante il processo di backup.

- Selezionare nella configurazione **Real-Time Protection > Scansione > Eccezioni** ed inserire i nomi di processo dei software di backup.

Il FireWall segnala Avira Real-Time Protection e Avira Mail Protection non appena sono attivi.

Causa: Avira Real-Time Protection e Avira Mail Protection comunicano tramite il protocollo Internet TCP/IP. Un firewall monitora tutte le connessioni mediante questo protocollo.

- Definire un permesso generale per Avira Real-Time Protection e Avira Mail Protection. Avira Real-Time Protection lavora esclusivamente con l'indirizzo 127.0.0.1 (localhost). Non viene stabilita alcuna connessione Internet. Altrettanto vale per Avira Mail Protection.

Avira Mail Protection non funziona.

✓ Verificare la funzionalità di Avira Mail Protection sulla base delle seguenti checklist se si manifestano problemi con Avira Mail Protection.

Checklist

✓ Verificare se il client mail si registra mediante Kerberos, APOP o RPA sul server. Questi metodi di autenticazione attualmente non vengono supportati.

✓ Verificare se il client mail viene registrato mediante SSL (spesso chiamato anche TSL - Transport Layer Security) sul server. Avira Mail Protection non supporta alcun SSL e chiude pertanto le connessioni SSL crittografate. Se si desidera utilizzare le connessioni SSL crittografate senza la protezione di Avira Mail Protection, per la connessione occorre usare una porta diversa da quelle controllate da Mail Protection. Le porte monitorate da Mail Protection possono essere configurate nella configurazione in **Mail Protection > Scansione**.

✓ Il servizio Avira Mail Protection (Service) è attivo? Eventualmente attivare il servizio: fare clic su **Start > Impostazioni >Pannello di controllo**. Fare doppio clic sulla finestra di configurazione **Servizi** per attivarla (in Windows XP l'applet dei servizi si trova nella sottocartella *Strumenti di amministrazione*). Cercare la voce *Avira Mail Protection*. Come modalità di avviamento deve essere inserito `Automatico` e come

stato `Avviato`. Avviare il servizio manualmente mediante la selezione della riga corrispondente e del pulsante **Avvia**. Se viene visualizzato un messaggio di errore, verificare la *visualizzazione eventi*. Se non si riesce, disinstallare completamente il prodotto Avira dal menu **Start > Impostazioni > Pannello di controllo > Software**, riavviare il computer e, infine, installare nuovamente il prodotto Avira.

Generale

- Mediante SSL (Secure Sockets Layer) le connessioni crittografate POP3 (spesso definite anche TLS - Transport Layer Security) in questo momento non possono essere protette e vengono ignorate.
- L'autenticazione al server mail attualmente viene supportata solo tramite password. Kerberos e RPA attualmente non sono supportati.
- Quando vengono inviate e-mail, il prodotto Avira non controlla la presenza di virus e programmi indesiderate.

> **Nota**
> Si consiglia di eseguire regolarmente gli aggiornamenti Microsoft per colmare le eventuali lacune in termini di sicurezza.

Un'e-mail inviata tramite una connessione TSL è stata bloccata da Mail Protection.

Causa: TLS (Transport Layer Security, il protocollo di codifica per la trasmissione dati su Internet) al momento non è supportato da Mail Protection. Per inviare l'e-mail è possibile:

- Utilizzare un'altra porta rispetto alla Porta 25 impegnata da SMTP. In questo modo si aggira la sorveglianza di Mail Protection.
- Rinunciare alla connessione codificata TSL e disattivare il supporto TSL nel client e-mail.
- Disattivare (ignorare) il monitoraggio delle e-mail in uscita da parte di Mail Protection in **Mail Protection > Scansione**.

La chat Web non funziona: i messaggi di chat non vengono visualizzati.

Questo fenomeno può verificarsi in chat che si basano sul protocollo HTTP con 'transfer-encoding= chunked'.

Causa: Web Protection controlla i dati inviati in modo completo alla ricerca di virus e programmi indesiderati prima che i dati siano caricati nel browser Web. Durante un trasferimento di dati con 'transfer-encoding= chunked', Web Protection non è in grado di rilevare la lunghezza dei messaggi o la quantità di dati.

- Nella configurazione impostare l'URL di Webchat come eccezione (vedere Configurazione: Web Protection > Scansione > Eccezioni).

15.2 Shortcut

Le shortcut offrono la possibilità di navigare velocemente nel programma, richiamare singoli moduli e avviare azioni.

Di seguito viene presentata una panoramica delle shortcut presenti disponibili. Per maggiori informazioni sulla funzionalità e disponibilità consultare il capitolo corrispondente della guida.

15.2.1 Nelle finestre di dialogo

Shortcut	Descrizione
Ctrl + Tab **Ctrl + Pggiù**	Navigazione in Control Center Passa alla rubrica successiva.
Ctrl + Maiusc + Tab **Ctrl + Pggiù**	Navigazione in Control Center Passa alla rubrica precedente.
←↑→↓	Navigazione nelle rubriche di configurazione Evidenzia con il mouse una rubrica di configurazione. Effettua una modifica tra le opzioni di un menu a tendina selezionate o tra più opzioni in un gruppo di opzioni.
Tab	Passa all'opzione successiva o al successivo gruppo di opzioni.
Maiusc + Tab	Passa all'opzione precedente o al precedente gruppo di opzioni.
Barra spaziatrice	Attiva o disattiva una casella di controllo se l'opzione attiva è una casella di controllo.
Alt + lettera sottolineata	Seleziona l'opzione o esegue il comando.
Alt + ↓ **F4**	Apre il menu a tendina selezionato.

Esc	Chiude il menu a tendina selezionato. Annulla il comando e chiude la finestra di dialogo.
Invio	Esegue comando per l'opzione o il pulsante attivo.

15.2.2 Nella Guida in linea

Shortcut	Descrizione
Alt + barra spaziatrice	Visualizza il menu del sistema.
Alt + Tab	Passa dalla Guida in linea ad altre finestre aperte.
Alt + F4	Chiude la Guida in linea.
Maiusc+ F10	Visualizza i menu contestuali della Guida in linea.
Ctrl + Tab	Passa alla rubrica successiva nella finestra di navigazione.
Ctrl + Maiusc + Tab	Passa alla rubrica precedente nella finestra di navigazione.
Pgsu	Passa all'argomento che è visualizzato sopra l'argomento attuale nel sommario, nell'indice o nell'elenco dei risultati della ricerca.
Pggiù	Passa all'argomento che è visualizzato sotto l'argomento attuale nel sommario, nell'indice o nell'elenco dei risultati della ricerca.
Pgsu **Pggiù**	Sfoglia le voci su un argomento.

15.2.3 In Control Center

Generale

Shortcut	Descrizione
F1	Visualizza la Guida in linea
Alt + F4	Chiude Control Center
F5	Aggiorna la visualizzazione
F8	Apre la configurazione
F9	Avvia aggiornamento

Rubrica **Scanner**

Shortcut	Descrizione
F2	Rinomina il profilo selezionato
F3	Avvia la scansione con il profilo selezionato
F4	Crea un collegamento sul desktop per il profilo selezionato
Agg	Crea un nuovo profilo
Canc	Elimina il profilo selezionato

Rubrica **Quarantena**

Shortcut	Descrizione
F2	Scansiona nuovamente l'oggetto
F3	Ripristina l'oggetto

F4	Invia l'oggetto
F6	Ripristina l'oggetto in...
Invio	Proprietà
Agg	Aggiungi file
Canc	Elimina l'oggetto

Rubrica **Pianificatore**

Shortcut	Descrizione
F2	Modifica del job
Invio	Proprietà
Agg	Inserisci nuovo job
Canc	Eliminazione del job

Rubrica **Report**

Shortcut	Descrizione
F3	Visualizza il file di report
F4	Stampa il file di report
Invio	Mostra il report
Canc	Elimina il report

Rubrica **Eventi**

Shortcut	Descrizione
F3	Esporta eventi
Invio	Mostra evento
Canc	Elimina evento

15.3 Centro sicurezza PC di Windows

- da Windows XP Service Pack 2 -

15.3.1 Generale

Il Centro sicurezza PC di Windows verifica lo stato di un computer dal punto di vista della sicurezza.

Se viene rilevato un problema in uno di questi punti importanti (ad esempio un programma antivirus vecchio), il Centro sicurezza PC invia un avviso e fornisce dei suggerimenti per proteggere più efficacemente il computer.

15.3.2 Centro sicurezza PC di Windows e il prodotto Avira in uso

Software di protezione antivirus/Protezione da software dannoso

È possibile ricevere i seguenti avvisi dal Centro sicurezza PC di Windows in relazione alla protezione antivirus:

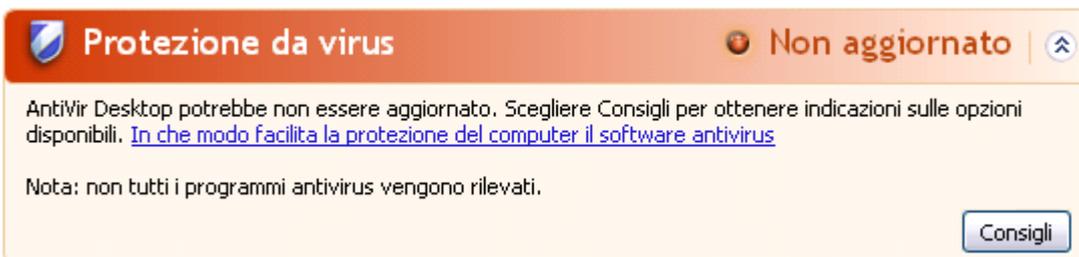
- Protezione antivirus NON TROVATA
- Protezione antivirus NON AGGIORNATA
- Protezione antivirus ATTIVA
- Protezione antivirus INATTIVA
- Protezione antivirus NON MONITORATA

Protezione antivirus NON TROVATA

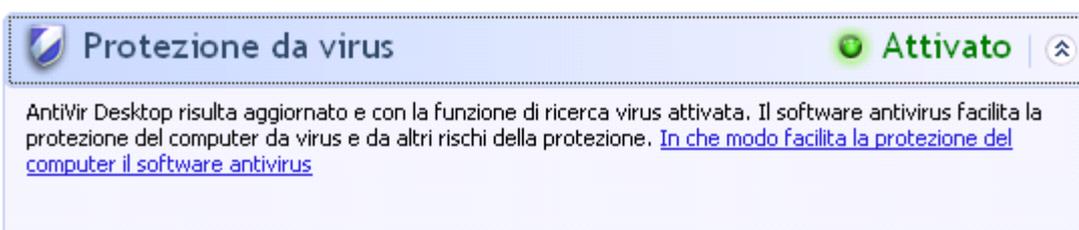
Questo avviso del Centro sicurezza PC di Windows viene visualizzato quando quest'ultimo non ha rilevato alcun software antivirus sul computer.

Nota
Installare il prodotto Avira in uso sul computer per proteggerlo da virus e altri programmi indesiderati.

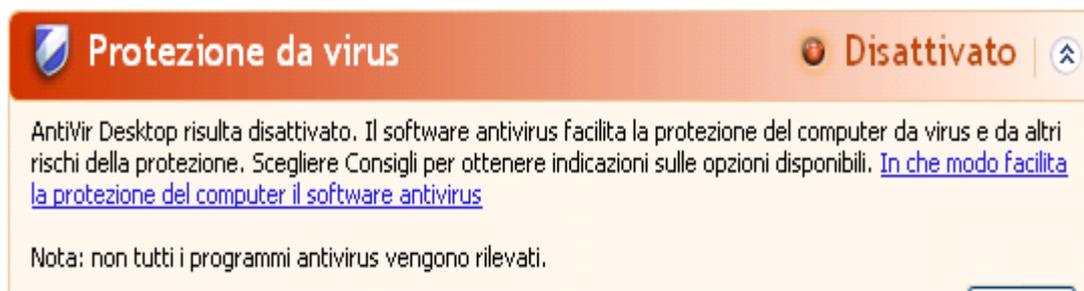
Protezione antivirus NON AGGIORNATA

Se si è già installato Windows XP Service Pack 2 e si installa successivamente il prodotto Avira oppure si installa Windows XP Service Pack 2 su un sistema in cui il prodotto Avira in uso è già installato, viene visualizzato il messaggio seguente:

Nota
Affinché il Centro sicurezza PC di Windows riconosca il prodotto Avira in uso come aggiornato, è necessario eseguire un aggiornamento dopo l'installazione. Aggiornare il sistema eseguendo un aggiornamento.

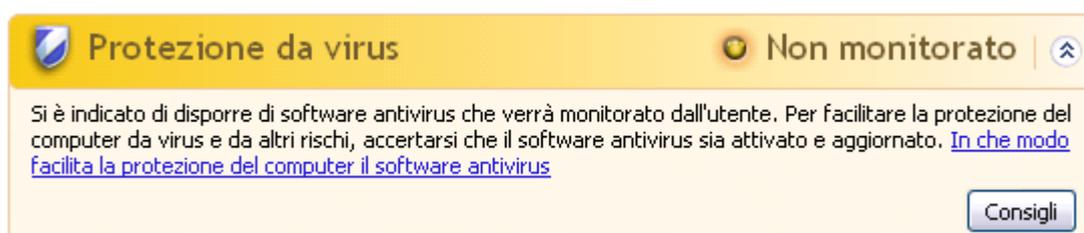
Protezione antivirus ATTIVA

Dopo l'installazione del prodotto Avira e un successivo aggiornamento viene visualizzato il messaggio seguente:

Il prodotto Avira è ora aggiornato e Avira Real-Time Protection è attivato.

Protezione antivirus INATTIVA

Il messaggio seguente viene visualizzato se si disattiva Avira Real-Time Protection o si interrompe il servizio Real-Time Protection.

> **Nota**
> È possibile attivare o disattivare Avira Real-Time Protection nella rubrica Stato di **Control Center**. Inoltre, è possibile vedere che Avira Real-Time Protection è attivo quando l'ombrello rosso nella barra delle applicazioni è aperto.

Protezione antivirus NON MONITORATA

Si riceve il seguente messaggio dal Centro sicurezza PC di Windows poiché si è optato per l'automonitoraggio del software antivirus.

> **Nota**
> Il Centro sicurezza PC di Windows è supportato dal prodotto Avira in uso. È possibile attivare questa opzione in ogni momento con il pulsante **Consigli...**.

> **Nota**
> Anche se Windows XP Service Pack 2 è installato, è comunque necessaria una soluzione antivirus. Sebbene Windows controlli il software antivirus non ha

alcuna funzione antivirus. L'utente non sarebbe protetto contro virus e malware senza una soluzione antivirus aggiuntiva.

15.4 Centro operativo di Windows

- Windows 7 e Windows 8 -

15.4.1 Generale

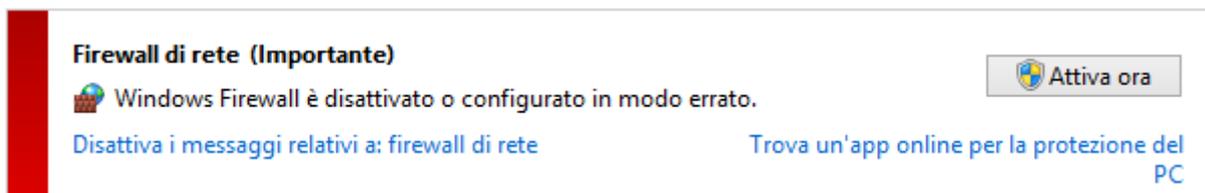
Nota:
Il **Centro sicurezza PC di Windows** ha assunto il nome **Centro operativo di Windows** a partire da Windows 7. Questa parte del programma indica lo stato di tutte le opzioni di sicurezza.

Il Centro operativo di Windows verifica lo stato di un computer dal punto di vista della sicurezza. È possibile accedere direttamente al Centro operativo facendo clic sulla bandierina nella barra delle applicazioni oppure su **Pannello di controllo > Centro operativo**.

Se viene rilevato un problema in uno di questi punti importanti (ad esempio un programma antivirus vecchio), il Centro operativo invia un avviso e fornisce dei suggerimenti per proteggere più efficacemente il computer. Ciò significa che, se tutto funziona correttamente, il Centro operativo non invia nessun avviso. È possibile tuttavia controllare lo stato di sicurezza del computer nel **Centro operativo** nella rubrica **Sicurezza**.
È possibile gestire e selezionare i programmi installati (ad esempio *visualizzare i programmi anti-spyware sul computer*).

Da **Centro operativo > Modifica impostazioni** è possibile disattivare i messaggi di avviso (ad esempio *Disattivazione dei messaggi per la sicurezza relativi a spyware e malware simili*).

15.4.2 Centro operativo di Windows e il prodotto Avira in uso

Windows Firewall è disattivato o non è configurato correttamente

- **Windows Firewall**

  A partire da Windows 7 Avira FireWall non è più contenuto in Avira Ultimate Protection Suite. È tuttavia possibile controllare Windows Firewall tramite il centro di controllo e configurazione.

Protezione antivirus

È possibile ricevere dal Centro operativo di Windows i seguenti avvisi sulla protezione antivirus:

- Avira Desktop ha segnalato che è installata la versione più recente e il riconoscimento dei virus è attivo
- Avira Desktop è disattivato
- Avira Desktop non è più aggiornato
- Sul computer non è stato trovato nessun software antivirus
- Il PC non è più protetto da Avira Desktop

Avira Desktop ha segnalato che la versione installata è la più recente e il riconoscimento dei virus è attivo

Dopo l'installazione del prodotto Avira e un successivo aggiornamento non viene visualizzato nessun messaggio dal Centro operativo di Windows. In **Centro operativo > Sicurezza** può comparire il seguente messaggio: *"Avira Desktop" ha segnalato che la versione installata è la più recente e il riconoscimento dei virus è attivo*. Questo significa che il prodotto Avira ora è aggiornato e Avira Real-Time Protection è attivo.

Avira Desktop è disattivato

Si riceve la seguente nota se si disattiva Avira Real-Time Protection o si arresta il servizio Real-Time Protection.

> **Nota**
> **Avira Real-Time Protection** può essere attivato o disattivato dalla rubrica **Stato** di **Avira Control Center**. Inoltre si può riconoscere se **Avira Real-Time Protection** è attivo quando l'ombrellino rosso nella barra delle applicazioni è aperto. È anche possibile attivare i singoli componenti Avira facendo clic sul pulsante *Attiva ora* del centro operativo. Se viene visualizzato un messaggio che richiede l'autorizzazione all'esecuzione del programma Avira, fare clic su *Consenti* per attivare Real-Time Protection.

Avira Desktop non è più aggiornato

Se Avira è già stato installato o se, per qualsiasi motivo, il file di definizione dei virus, il motore di ricerca o i programmi del prodotto Avira non vengono aggiornati automaticamente (ad es. quando si esegue l'upgrade da una versione precedente di un

sistema operativo Windows in cui è già installato il prodotto Avira a una nuova versione), si riceve il seguente messaggio:

Protezione da virus (Importante)
Avira Desktop non è aggiornato.
Disattiva i messaggi relativi a: protezione da virus
Aggiorna ora
Recuperare un altro programma antivirus online

> **Nota**
> Per far sì che il Centro operativo di Windows riconosca il prodotto Avira come aggiornato, dopo l'installazione è necessario eseguire un aggiornamento. Aggiornare il sistema eseguendo un aggiornamento.

Sul computer non è stato trovato nessun software antivirus

Questo avviso del Centro operativo di Windows viene visualizzato quando quest'ultimo non ha rilevato alcun software antivirus sul computer.

Protezione da virus (Importante)
Impossibile trovare software antivirus installato nel computer.
Disattiva i messaggi relativi a: protezione da virus
Trova programma online

> **Nota**
> Tenere presente che questa opzione non è disponibile in Windows 8. In questo sistema operativo Windows Defender è la funzione antivirus preconfigurata di Microsoft.
>
> **Nota**
> Installare sul computer il prodotto Avira in uso per proteggerlo da virus e altri programmi indesiderati!

Il PC non è più protetto da Avira Desktop

Questa nota del Centro operativo di Windows viene visualizzata alla scadenza della licenza del prodotto Avira.
Se si fa clic sul pulsante **Esegui azione**, si accede al sito Web Avira in cui è possibile acquistare una nuova licenza.

Protección antivirus (Importante)
Avira Desktop dejó de proteger el equipo.
Desactivar mensajes sobre protección antivirus
Tomar medidas
Ver aplicaciones antivirus instaladas

> **Nota**
> Tenere presente che questa opzione è disponibile solo per Windows 8.

Protezione da spyware e software indesiderati

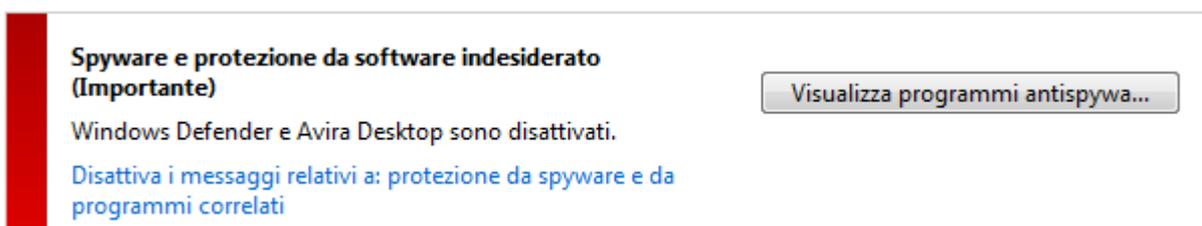
È possibile ricevere i seguenti avvisi dal Centro operativo di Windows in relazione alla protezione da spyware e software indesiderati:

- Avira Desktop ha segnalato che è attivo
- Windows Defender e Avira Desktop sono disattivati
- Avira Desktop non è più aggiornato
- Windows Defender non è più aggiornato
- Windows Defender è disattivato

Avira Desktop ha segnalato che è attivo

Dopo l'installazione del prodotto Avira e un successivo aggiornamento non viene visualizzato nessun messaggio dal Centro operativo di Windows. In **Centro operativo > Sicurezza** può comparire il seguente messaggio: *"Avira Desktop" ha segnalato che è attivo*. Questo significa che il prodotto Avira ora è aggiornato e Avira Real-Time Protection è attivo.

Windows Defender e Avira Desktop sono disattivati

Il seguente messaggio viene visualizzato se si disattiva Avira Real-Time Protection o si arresta il servizio Avira Real-Time Protection.

Spyware e protezione da software indesiderato (Importante)
Windows Defender e Avira Desktop sono disattivati.
Disattiva i messaggi relativi a: protezione da spyware e da programmi correlati
Visualizza programmi antispywa...

> **Nota**
> **Avira Real-Time Protection** può essere attivato o disattivato dalla rubrica **Stato** di **Avira Control Center**. Inoltre si può riconoscere se **Avira Real-Time Protection** è attivo quando l'ombrellino rosso nella barra delle applicazioni è aperto. È anche possibile attivare i singoli componenti Avira facendo clic sul pulsante *Attiva ora* del centro operativo. Se viene visualizzato un messaggio che richiede l'autorizzazione all'esecuzione del programma Avira, fare clic su *Consenti* per attivare Real-Time Protection.

Avira Desktop non è più aggiornato

Se Avira è già stato installato o se, per qualsiasi motivo, il file di definizione dei virus, il motore di ricerca o i programmi del prodotto Avira non vengono aggiornati automaticamente (ad es. quando si esegue l'upgrade da una versione precedente di un sistema operativo Windows in cui è già installato il prodotto Avira a una nuova versione), si riceve il seguente messaggio:

Nota
Per far sì che il Centro operativo di Windows riconosca il prodotto Avira come aggiornato, dopo l'installazione è necessario eseguire un aggiornamento. Aggiornare il sistema eseguendo un aggiornamento.

Windows Defender non è più aggiornato

Il seguente messaggio può essere visualizzato se Windows Defender è attivo. Ciò potrebbe significare che il prodotto Avira in uso non è stato installato correttamente. Controllare.

Nota
Windows Defender è la soluzione antivirus e di protezione da spyware predefinita di Windows.

Windows Defender è disattivato

Il messaggio del Centro operativo di Windows *Windows Defender è disattivato* viene visualizzato se sul computer non sono stati trovati altri software anti-spyware. Windows Defender è un software per il riconoscimento degli spyware di Microsoft integrato nel sistema operativo. Se sul computer è già stato installato un altro software antivirus, quest'applicazione viene disattivata.
Se il prodotto Avira è installato correttamente questo messaggio non dovrebbe comparire, perché il Centro operativo riconosce automaticamente Avira. Controllare se Avira funziona correttamente.

16. Virus e altro

Avira Ultimate Protection Suite non si limita al riconoscimento di virus e malware, ma può anche proteggere da altri rischi. In questo capitolo viene presentata una panoramica dei diversi tipi di malware e degli altri rischi. Viene descritta la loro provenienza e il loro comportamento, nonché le spiacevoli sorprese che possono causare.

Argomenti correlati:

- Categorie di minacce
- Virus e altri malware

16.1 Categorie di minacce

Adware

Con Adware si designa un software che mostra all'utente i banner e i popup pubblicitari. Questi inserti pubblicitari generalmente non possono essere chiusi e sono quasi sempre visibili. I dati della connessione permettono numerosi feedback sul comportamento dell'utente e sono problematici per motivi di sicurezza dei dati.

Il prodotto Avira riconosce gli adware. Se nella configurazione in Categorie di minacce l'opzione **Adware** è attivata, si riceve un avviso quando il prodotto Avira rileva un software di questo tipo.

Adware/Spyware

Software che visualizza messaggi pubblicitari o che invia i dati personali dell'utente, spesso a sua insaputa, a terzi e che risulta quindi indesiderato.

Il prodotto Avira riconosce gli Adware/Spyware. Se nella configurazione in Categorie di minacce l'opzione **Adware/Spyware** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira esegue un rilevamento.

Applicazione

Per applicazione si intende un'applicazione il cui utilizzo può essere rischioso o la cui origine è dubbia.
Il prodotto Avira riconosce l'Applicazione (APPL). Se nella configurazione in Categorie di minacce l'opzione **Applicazione** è attivata con un segno di spunta, si riceve un avviso se il prodotto Avira effettua un rilevamento.

Software di controllo backdoor

Per prelevare dati o manipolare il sistema viene inserito dalla porta posteriore un programma server backdoor senza che l'utente se ne accorga. Questo programma può essere gestito da terzi mediante Internet o la rete con un software di gestione backdoor (Client).
Il prodotto Avira riconosce i software di controllo backdoor. Se nella configurazione in Categorie di minacce l'opzione **Software di controllo backdoor** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira esegue un rilevamento.

File con estensioni occultate

File eseguibili che occultano la propria estensione in modo sospetto. Il metodo dell'occultamento viene spesso utilizzato dai malware.
Il prodotto Avira riconosce i file con estensioni occultate. Se nella configurazione in Categorie di minacce l'opzione **File con estensioni occultate** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

Programma di selezione a pagamento

Alcuni servizi offerti in Internet sono a pagamento. In Germania la fatturazione avviene per programmi di selezione con i numeri 0190/0900 (in Austria e Svizzera con i numeri 09x0; in Germania a medio termine passerà ai numeri 09x0). Se installati sul computer, questi programmi (dialer) garantiscono la creazione della connessione mediante i numeri Premium-Rate, la cui tariffa può variare enormemente.

La commercializzazione di contenuti online mediante la bolletta telefonica è legale e può essere vantaggiosa per l'utente. I dialer seri non hanno alcun dubbio sul fatto che il cliente sia consapevole e lo utilizzi in modo avveduto. Tali contenuti si installano sul computer dell'utente solo se l'utente dà la propria approvazione, espressa sulla base di un'etichettatura ben riconoscibile o di una richiesta univoca e chiara. La creazione della connessione di programmi dialer seri viene visualizzata in maniera chiara e non ambigua. Inoltre, i dialer seri informano l'utente in maniera esatta e precisa sui costi correlati.

Purtroppo però esistono dialer che si installano senza farsi notare, in maniera dubbia o addirittura fraudolenta. Sostituiscono, ad esempio, la connessione standard dial up dell'utente di Internet all'ISP (Internet-Service-Provider) e a ogni connessione selezionano numeri a pagamento spesso estremamente costosi, come i numeri 0190/0900. L'utente interessato nota dalla bolletta successiva che è stato installato un programma dialer indesiderato che si connette a ogni accesso a Internet ai numeri a pagamento 0190/0900, facendo salire in modo esorbitante la bolletta.

Per proteggersi da programmi di selezione non desiderati e a pagamento (dialer 0190/0900), consigliamo di rivolgersi direttamente al proprio gestore telefonico per bloccare questo tipo di numeri.

Di default, il prodotto Avira riconosce i programmi di selezione a pagamento a lui noti.

Se nella configurazione di Categorie di minacce è stata attivata l'opzione **Programmi di selezione a pagamento** con un segno di spunta, in caso di rilevamento di un programma di selezione a pagamento viene emesso un messaggio di avviso. Si ha quindi la possibilità di eliminare facilmente gli eventuali dialer indesiderati per i numeri 0190/0900. Se si tratta di un programma di selezione a pagamento voluto, si può dichiarare un file da escludere che non verrà più scansionato in futuro.

Phishing

Il phishing, anche noto come brand spoofing è una forma raffinata di furto dei dati per i clienti o i potenziali clienti di provider Internet, banche, servizi di banking online, enti di registrazione.
Con la trasmissione dell'indirizzo e-mail in Internet, la compilazione di moduli online, la partecipazione a newsgroup o siti Web, è possibile che vengano sottratti i dati dai cosiddetti Internet crawling spiders e utilizzati senza autorizzazione per frodi o altre attività illegali.

Il prodotto Avira riconosce il phishing. Se nella configurazione in Categorie di minacce l'opzione **Phishing** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

Programmi che violano la privacy dell'utente

Software che minano la sicurezza del sistema, causano funzioni di programma non desiderate, violano la sfera privata o spiano il comportamento dell'utente e che sono quindi generalmente indesiderati.

Il prodotto Avira riconosce i software che mettono a repentaglio la sicurezza. Se nella configurazione in Categorie di minacce l'opzione **Programmi che violano la privacy dell'utente** è attivata con un segno di spunta, si riceve un avviso se il prodotto Avira ha eseguito un rilevamento.

Programmi ludici

I programmi ludici possono inorridire qualcuno o divertire tutti, senza essere dannosi o moltiplicarsi. La maggior parte delle volte il computer dopo il richiamo del programma ludico inizia a far suonare una melodia o a visualizzare qualcosa di insolito sullo schermo. Esempi di programmi ludici sono le lavatrici nel drive del floppy disk (DRAIN.COM) o il divoraschermo (BUGSRES.COM).

Ma attenzione! Tutte le manifestazioni di un programma ludico potrebbero anche essere prodotte da un virus o un trojan. L'effetto minimo sull'utente è uno spavento ma si può anche andare nel panico per la paura dei danni che possono verificarsi.

Il prodotto Avira è in grado di riconoscere i programmi ludici mediante un'estensione delle proprie routine di scansione ed eventualmente di eliminare il programma indesiderato. Se nella configurazione in Categorie di minacce è stata selezionata l'opzione **Programmi ludici** con un segno di spunta, si viene informati sui relativi rilevamenti.

Giochi

I giochi per computer devono esistere, ma non necessariamente sul luogo di lavoro (ad eccezione a volte della pausa pranzo). Tuttavia i dipendenti delle aziende e i collaboratori degli enti pubblici spesso usano i giochi. Su Internet sono disponibili moltissimi giochi. Anche i giochi tramite e-mail stanno prendendo piede: dal semplice gioco degli scacchi a battaglia navale (con tanto di battaglie con torpedo), sono numerose le varianti in circolazione. Le mosse vengono inviate e ricevute mediante il programma di posta elettronica.

Alcune ricerche hanno dimostrato che il tempo durante l'orario lavorativo dedicato ai giochi per computer sta assumendo proporzioni rilevanti. Pertanto è comprensibile che sempre più aziende prendano in considerazione la possibilità di eliminare i giochi dai computer utilizzati per lavoro.

Il prodotto Avira riconosce i giochi per computer. Se nella configurazione in Categorie di minacce l'opzione **Giochi** è attivata con un segno di spunta, si riceve un avviso se il prodotto Avira ha eseguito un rilevamento. Il gioco è finito nel vero senso della parola visto che è possibile escluderlo facilmente.

Software ingannevole

Noti anche con il nome di Scareware (programmi spaventosi) o Rogueware (programmi canaglia), sono software ingannevoli che simulano infezioni di virus e rischi e quindi sono ingannevolmente simili ai software antivirus professionali. Gli scareware mirano a disorientare o spaventare l'utente. Se la vittima cade nel trabocchetto e si sente minacciata, gli viene offerta una soluzione (spesso a pagamento) per rimuovere la minaccia inesistente. In altri casi la vittima, credendo che sia avvenuto un attacco, viene indotta a intraprendere azioni che rendono possibile l'attacco vero e proprio.

Se nella configurazione di Categorie di minacce è stata attivata l'opzione **Software ingannevole** con un segno di spunta, in caso di rilevamento di uno scareware viene emesso un messaggio di avviso.

Programmi di compressione runtime insoliti

I file compressi con un programma di compressione runtime insolito possono essere identificati come sospetti.

Il prodotto Avira riconosce gli strumenti di compressione runtime insoliti. Se nella configurazione in Categorie di minacce l'opzione **Strumento di compressione runtime insolito** è attivata con un segno di spunta, si riceve un avviso quando il prodotto Avira effettua un rilevamento.

16.2 Virus e altri malware

Adware

Con Adware si designa un software che mostra all'utente i banner e i popup pubblicitari. Questi inserti pubblicitari generalmente non possono essere chiusi e sono quasi sempre visibili. I dati della connessione permettono numerosi feedback sul comportamento dell'utente e sono problematici per motivi di sicurezza dei dati.

Backdoor

Un backdoor (in italiano porta posteriore) permette, aggirando la tutela all'accesso, di ottenere l'accesso a un computer.

Un programma in esecuzione di nascosto permette a un aggressore di godere di diritti pressoché illimitati. Con l'aiuto del backdoor i dati personali dell'utente possono essere spiati. I backdoor però vengono utilizzati soprattutto per installare altri virus o worm sul sistema infetto.

Virus dei record di avvio

Il record di avvio e il record master di avvio degli hard disk vengono inficiati di preferenza da virus dei record di avvio, che sovrascrivono informazioni importanti all'avvio del sistema. Una delle spiacevoli conseguenze è che il sistema operativo non può più essere caricato...

Bot-Net

Per Bot-Net si intende una rete di PC gestibile a distanza (in Internet), composta da bot che comunicano l'uno con l'altro. Questo controllo si raggiunge con virus e trojan che inficiano il computer e poi aspettano indicazioni senza apportare danni al computer intaccato. Queste reti possono essere utilizzare per la diffusione di spam, attacchi DDoS, ecc., talvolta senza che gli utenti del PC si accorgano di alcunché. Il potenziale principale dei Bot-Net è quello di poter raggiungere reti di migliaia di computer, la cui portata salta gli accessi a Internet.

Exploit

Un Exploit (lacuna di sicurezza) è un programma del computer o uno script che sfrutta le debolezze specifiche o le funzioni errate di un sistema operativo o del programma. Una forma di Exploit sono gli attacchi da Internet con l'aiuto di pacchetti di dati manipolati, che sfruttano le debolezze nel software di rete. Con l'utilizzo di alcuni programmi che si introducono clandestinamente si ottiene un più ampio accesso.

Hoaxes (in inglese hoax: scherzo, burla)

Da un paio di anni gli utenti ricevono avvisi di virus che potrebbero diffondersi per e-mail in Internet o in altre reti. Questi avvisi vengono distribuiti via e-mail con la richiesta di inoltrarli a quanti più colleghi possibili per mettere tutti in guardia dal "pericolo".

Honeypot

Un Honeypot (pentola di miele) è un servizio installato in una rete (programma o server). Esso ha il compito di monitorare una rete e registrare gli attacchi. Questo servizio è sconosciuto all'utente legittimo e quindi non viene mai toccato. Quando un aggressore cerca punti di debolezza in una rete e prende in considerazione i servizi offerti da un Honeypot, viene registrato e viene emesso un allarme.

Macrovirus

I macrovirus sono piccoli programmi che sono scritti nella lingua delle macro di un'applicazione (ad esempio WordBasic in WinWord 6.0) e normalmente potrebbero diffondersi all'interno di documenti di questa applicazione. Essi vengono pertanto chiamati anche virus dei documenti. Per renderli attivi è necessario avviare l'applicazione corrispondente ed eseguire una delle macro infette. Diversamente dai virus "normali", i macrovirus non riguardano i file eseguibili, bensì i documenti dell'applicazione host.

Pharming

Il pharming è una manipolazione del file host dei browser Web, per reindirizzare richieste dei siti Web falsificati. Si tratta di una rielaborazione del classico phishing. I truffatori che si servono del pharming godono di grandi quantità di server sui quali vengono archiviati i siti Web falsificati. Il pharming si è consolidato come iperonimo per diversi tipi di attacchi al DNS. In caso di manipolazione del file host con l'ausilio di un trojan o un virus viene effettuata una manipolazione del sistema. La conseguenza è che sono richiamabili solo siti Web falsificati da questo sistema, se l'indirizzo Web viene inserito correttamente.

Phishing

Phishing significa letteralmente pescare dati personali degli utenti di Internet. Il phisher invia generalmente alla vittima lettere aventi valore ufficiale, come ad esempio e-mail che veicolano informazioni sensibili, soprattutto nomi utente e password o PIN e TAN di accessi all'Online Banking, approfittando della buona fede dell'utente. Con i dati di accesso rubati il phisher assume l'identità della vittima e conduce operazioni a suo nome. Va precisato che le banche e le assicurazioni non chiedono mai di inviare numeri di carte di credito, PIN, TAN o altri dati di accesso per e-mail, SMS o telefonicamente.

Virus polimorfi

I veri campioni del mimetismo e del travestimento sono i virus polimorfi. Modificano i propri codici di programmazione e sono quindi particolarmente difficili da riconoscere.

Virus di programma

Un virus del computer è un programma che ha la capacità, una volta richiamato, di agganciarsi in qualche modo ad altri programmi e, da tale posizione, di inficiare il sistema. I virus si diffondono quindi in contrasto alle bombe logiche e ai trojan stessi. Al contrario di un worm, un virus ha bisogno di un programma estraneo ospite in cui archiviare il proprio codice virulento. Normalmente, tuttavia, la funzionalità del programma ospite non viene modificata.

Rootkit

Per rootkit si intende un insieme di strumenti software che vengono installati su un computer dopo un'irruzione per nascondere il login dell'intruso, nascondere processi e registrare dati, in linea generale: per rendersi invisibili. I rootkit tentano di aggiornare i programmi spia già installati e di installare nuovamente gli spyware eliminati.

Virus di script e worm

Questi virus sono estremamente semplici da programmare e in poche ore si diffondono per e-mail a livello globale, premesso che siano presenti tecniche ad hoc.

I virus di script e i worm utilizzano la lingua degli script, come ad esempio Javascript, VBScript ecc., per inserirsi in altri nuovi script o per diffondersi mediante il richiamo di funzioni del sistema operativo. Spesso ciò avviene tramite e-mail o mediante lo scambio di file (documenti).

Il worm è un programma che non intacca alcun documento ospite. I worm non possono quindi divenire un componente di altri programmi. I worm rappresentano spesso l'unica possibilità di introdursi clandestinamente su sistemi dotati di provvedimenti restrittivi legati alla sicurezza.

Spyware

Gli spyware sono i cosiddetti programmi spia che inviano dati personali dell'utente a terzi senza che questi ne siano a conoscenza e senza l'approvazione del produttore del software. I programmi spyware servono soprattutto ad analizzare la navigazione in Internet e a introdurre banner o popup pubblicitari in maniera mirata.

Cavalli di Troia (in breve trojan)

I trojan sono sempre più diffusi. Così vengono definiti i programmi che pretendono di avere una funzione precisa; dopo il loro avvio, tuttavia, mostrano il loro vero volto ed eseguono altre funzioni che hanno per lo più effetti distruttivi. I trojan non possono moltiplicarsi da soli e in questo si differenziano dai virus e dai worm. La maggior parte di loro ha un nome interessante (SEX.EXE o STARTME.EXE), che ha la funzione di spingere l'utente a eseguire il trojan. Subito dopo l'esecuzione diventano attivi e formattano, ad esempio, l'hard disk. Un tipo particolare di trojan è il dropper, che "lascia cadere" i virus, ovvero li installa nel sistema del computer.

Software ingannevole

Noti anche con il nome di Scareware (programmi spaventosi) o Rogueware (programmi canaglia), sono software ingannevoli che simulano infezioni di virus e rischi e quindi sono ingannevolmente simili ai software antivirus professionali. Gli scareware mirano a disorientare o spaventare l'utente. Se la vittima cade nel trabocchetto e si sente minacciata, gli viene offerta una soluzione (spesso a pagamento) per rimuovere la minaccia inesistente. In altri casi la vittima, credendo che sia avvenuto un attacco, viene indotta a intraprendere azioni che rendono possibile l'attacco vero e proprio.

Zombie

Un PC zombie è un computer che viene intaccato da programmi malware e permette all'hacker di abusare del computer in remoto per fini criminali. Il PC infetto lancia il comando, ad esempio, di attacchi di Denial-of-Service- (DoS) o invia spam o e-mail di phishing.

17. Info e Service

Questo capitolo contiene informazioni relative a Info e Service Avira.

- Indirizzi di contatto
- Supporto tecnico
- File sospetto
- Comunicazione di un falso allarme
- Feedback per migliorare la sicurezza

17.1 Indirizzi di contatto

Siamo a disposizione del cliente qualora avesse domande o suggerimenti sul mondo dei prodotti Avira Ultimate Protection Suite. I nostri recapiti sono disponibili in Control Center alla voce **Guida > Informazioni su Avira Ultimate Protection Suite**.

17.2 Supporto tecnico

Il supporto Avira è rivolto all'utente, serve a rispondere alle sue domande o a risolvere un problema tecnico.

Tutte le informazioni necessarie relative al nostro servizio di supporto completo sono disponibili sul sito Web:

http://www.avira.com/it/support

Per poter ricevere aiuto nel modo migliore e più veloce possibile, occorre tenere a portata di mano le seguenti informazioni:

- **Dati sulla licenza**. Si trovano sull'interfaccia del programma nella voce di menu **Guida in linea > Informazioni su Avira Ultimate Protection Suite > Informazioni sulla licenza**. Vedere Informazioni sulla licenza.
- **Informazioni sulla versione**. Si trovano sull'interfaccia del programma nella voce di menu **Guida in linea > Informazioni su Avira Ultimate Protection Suite > Informazioni sulla versione**. Vedere Informazioni sulla versione.
- **Versione del sistema operativo** e service pack eventualmente installati.
- **I pacchetti software installati**, ad esempio software antivirus di altri produttori.
- **Messaggi precisi** del programma o del file di report.

17.3 File sospetto

I file sospetti o i virus che non possono essere riconosciuti o eliminati dai nostri prodotti possono essere inviati a noi. A tale scopo sono disponibili diverse modalità di invio.

- Identificare il file nel manager della quarantena di Control Center della Server Security Console Avira e selezionare l'elemento **Invia file** dal menu contestuale o con il pulsante corrispondente.
- Inviare il file desiderato in formato compresso (WinZIP, PKZip, Arj, ecc.) come allegato a un'e-mail al seguente indirizzo:
  virus@avira.com
  Poiché alcuni gateway di posta elettronica operano con software antivirus, si prega di proteggere il file/i file con una password (non dimenticare di comunicare anche la password).
- In alternativa è possibile inviare il file sospetto mediante la nostra pagina Web:
  http://www.avira.com/sample-upload

17.4 Comunicazione di un falso allarme

Se si ritiene che Avira Ultimate Protection Suite stia comunicando un rilevamento di un file probabilmente "pulito", inviare tale file compresso (WinZIP, PKZip, Arj, etc.) come allegato a un'email al seguente indirizzo:

virus@avira.com

Poiché alcuni gateway di posta elettronica operano con software antivirus, si prega di proteggere il file/i file con una password (non dimenticare di comunicare anche la password).

17.5 Feedback per migliorare la sicurezza

Per Avira la sicurezza degli utenti è al primo posto. Pertanto non disponiamo solamente di un team di esperti, a cui viene sottoposta ogni singola soluzione Avira e ogni aggiornamento prima della pubblicazione dei test di sicurezza e qualità. Il nostro lavoro consiste anche nel prendere seriamente le note su eventuali punti di debolezza rilevanti per la sicurezza e nell'affrontarle apertamente.

Se si ritiene che esista una lacuna rilevante per la sicurezza in uno dei nostri prodotti, inviare un'e-mail al seguente indirizzo:

vulnerabilities@avira.com